NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ACHIEVING INFORMATION SUPERIORITY USING HASTILY FORMED NETWORKS AND EMERGING TECHNOLOGIES FOR THE ROYAL THAI ARMED FORCES COUNTERINSURGENCY OPERATIONS IN SOUTHERN THAILAND

by

Anthony A. Bumatay
Grant Graeber

March 2014

Thesis Co-Advisor: Brian Steckler
Thesis Co-Advisor: Edward Fisher

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
ACHIEVING INFORMATION SUPERIORITY USING HASTILY FORMED NETWORKS AND EMERGING TECHNOLOGIES FOR THE ROYAL THAI ARMED FORCES COUNTERINSURGENCY OPERATIONS IN SOUTHERN THAILAND

5. FUNDING NUMBERS

6. AUTHOR(S) Anthony A. Bumatay and Grant Graeber

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The southern Thailand provinces of Yala, Pattani, Narathiwat and Songkhla have seen a resurgence in Malay-Muslim violence since 2004. The scale and level of sophistication of the insurgent attacks have caused instability in the region and disruption in a country already marred by political turmoil. This thesis examines the history, trends in violence and actors behind the Malay-Muslim insurgency as well as the effectiveness of the Royal Thai Armed Forces' counterinsurgency response. This is to create an analytical context that may be useful in the current Royal Thai Armed Forces (RTARF) approach in southern Thailand.

This thesis also explores the applicability of network centric technologies such as hastily formed networks (HFN) as the backbone of a technological framework that will deliver information superiority to enable the Thai government to gain a tactical edge against the insurgent movement in southern Thailand. Along with the HFN concept, an overview of the emerging technologies that were demonstrated during the U.S.-Thailand Crimson Viper technology demonstration in Hat Yao, Thailand from August 1–9, 2013, are provided. This discussion will show how alternative power sources, social network analysis, persistent surveillance systems and unmanned vehicles, if integrated with HFN wireless ad hoc networking, provides an effective model to support the RTARF's counterinsurgency operations in southern Thailand.

14. SUBJECT TERMS Insurgency, Counterinsurgency, Hastily Formed Networks, Lighthouse, Networking, Muslim, Islam, Terrorism, network centric warfare, Network Operations, Pattani, Naratiwat, Yala	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

ACHIEVING INFORMATION SUPERIORITY USING HASTILY FORMED NETWORKS AND EMERGING TECHNOLOGIES FOR THE ROYAL THAI ARMED FORCES COUNTERINSURGENCY OPERATIONS IN SOUTHERN THAILAND

Anthony A. Bumatay
Lieutenant Commander, United States Navy
B.S., De La Salle University, 1994
M.S., University of San Francisco, 2002

Grant Graeber
Lieutenant, United States Navy
B.S., United States Naval Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2014

Author: Anthony A. Bumatay
Grant Graeber

Approved by: Brian Steckler
Thesis Co-Advisor

Edward Fisher
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The southern Thailand provinces of Yala, Pattani, Narathiwat and Songkhla have seen a resurgence in Malay-Muslim violence since 2004. The scale and level of sophistication of the insurgent attacks have caused instability in the region and disruption in a country already marred by political turmoil. This thesis examines the history, trends in violence and actors behind the Malay-Muslim insurgency as well as the effectiveness of the Royal Thai Armed Forces' counterinsurgency response. This is to create an analytical context that may be useful in the current Royal Thai Armed Forces (RTARF) approach in southern Thailand.

This thesis also explores the applicability of network centric technologies such as hastily formed networks (HFN) as the backbone of a technological framework that will deliver information superiority to enable the Thai government to gain a tactical edge against the insurgent movement in southern Thailand. Along with the HFN concept, an overview of the emerging technologies that were demonstrated during the U.S.-Thailand Crimson Viper technology demonstration in Hat Yao, Thailand from August 1–9, 2013, are provided. This discussion will show how alternative power sources, social network analysis, persistent surveillance systems and unmanned vehicles, if integrated with HFN wireless ad hoc networking, provides an effective model to support the RTARF's counterinsurgency operations in southern Thailand.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BERSATU	Barisan Bersatu Kemerdekaan Pattani
BGAN	Broadband Global Area Network
BNPP	Barisan National Pember-Basan Pattani
BRN-C	Barisan Revolusi Nasional Coordinate
C2	command and control
CIA	Central Intelligence Agency
CINC	Commander In Chief
C-IED	counter improvised explosive device
COP	common operational picture
CORE	Common Operational Research Environment
COTS	commercial off the shelf
CPM	civil-police military
CV13	Crimson Viper 2013
EBO	effects based operations
GEOINT	geospatial intelligence
GMIP	Garakan Mujahidin Islam Patani
GMP	Gerakan Mujahideen Pattani
GSM	Global System for Mobile
FSS	fixed satellite system
HADR	humanitarian assistance and disaster relief
HFN	hastily formed networks
HUMINT	human intelligence
IED	improvised explosive device
ICT	information communications technology
IM	information management
ISOC	Internal Security Operations Command
JEM	Justice and Equality Movement
KBPS	kilobits per second
LGU	local government unit
MANET	mobile ad hoc networking

MBPS	megabits per second
MCP	Malayan Communist Party
MEC	MarForPac Experimentation Center
MKO	Mujahidine Khalq
NCW	Network Centric Warfare
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NGO	non-governmental organization
NPLF	National Pattani Liberation Front
NPS	Naval Postgraduate School
OTH	over the horizon
PGSS	persistent ground surveillance system
PGST	persistent ground surveillance tower
PULO	Patani United Liberation Organization
RENEWS	Reusing Existing Natural Energy, Wind and Solar
RMA	revolution in military affairs
RTAF	Royal Thai Air Force
RTARF	Royal Thai Armed Forces
RTN	Royal Thai Navy
RUF	Revolutionary United Front
SBPAC	Southern Border Provinces Administrative Charter
SBPPC	Southern Border Provinces Peace Building Command
SLA	Sudan Liberation Army
SNA	social network analysis
UAV	unmanned aerial vehicle
UGV	unmanned ground vehicle
VDV	village defense volunteers
VSAT	very small aperture terminal
VSO	village stability operations
VSP	village stability platform
WIMAX	worldwide interoperability for microwave access
WSN	wireless sensor network

ACKNOWLEDGMENTS

We would like to express our sincerest gratitude to our two thesis advisors, professors Brian Steckler and Edward Fisher, who painstakingly guided us through months of research and editing. Without their professional support, this thesis would not have been possible. Being part of the Hastily Formed Networks research group has been a wonderful experience as it provided us with a unique opportunity to participate in overseas engagements such as Crimson Viper 2013 in Thailand and Operation Damayan, the U.S. military's HA/DR response to super typhoon Haiyan's aftermath in the Philippines. Brian, you are not only an amazing thesis advisor, but a great friend and mentor. We would also like to take this opportunity to thank the U.S. Navy for giving us the chance to further our knowledge and gain valuable insight from the outstanding faculty at the Naval Postgraduate School. This educational experience has been an amazing endeavor and we hope to apply this new insight upon our return to the fleet. Last, we would like to thank our families and their unrelenting support to help us through this academic journey.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Since 2004, the Malay-Muslim insurgency in Thailand's southernmost provinces of Yala, Pattani, Narathiwat and Songkhla has escalated. The scale and level of sophistication of these insurgent attacks have captured both national and international attention, causing obvious disruption within the country and instability in the region. According to the 2011 report *Ongoing Insurgency in Southern Thailand: Trends in Violence and Counterinsurgency Operations*, published by the Institute for National Strategic Studies, the current conflict has claimed more than 4,500 lives and another 9,000 people were wounded. A monthly average of 32 deaths and 58 wounded make the ongoing insurgency in southern Thailand the deadliest in Southeast Asia. Most of the casualties are a result of improvised explosive device (IED) attacks, which average about 12 per month (Abuza, 2011).

The Thai central government has been unsuccessful in dealing with the insurgency even as new policies are implemented and additional organizations are created to confront this problem. In particular, the government has been hampered by unreliable intelligence and insufficient information to pursue and prosecute the insurgent leaders. The lack of intelligence also has undermined any chance for timely warnings about attacks.

RTARF intelligence operations rely almost exclusively on human intelligence (HUMINT) that is sourced from informants, village surveys, interrogations as well as interviews. This intelligence gathering approach is mostly unreliable and does not provide the critical information to make an immediate and effective operational impact. These issues are critical in resolving the problem and preventing the loss of innocent human lives.

For an effective counterinsurgency (COIN) framework in southern Thailand to work, emerging technology should be at the forefront of operations with a particular

emphasis on network centric operations that enable expeditious and effective collection of data for superior decision-making to defeat the adversary.

B. PROBLEM STATEMENT

The problem is the absence of a robust technology framework that provides the collection and dissemination of accurate and real-time information, common operational picture (COP) capabilities and decision-support tools that effectively address Thailand's southern insurgency problem. The Royal Thai Armed Forces' sole use of human intelligence (HUMINT) through informants does not provide the speed, precision and operational intelligence necessary to make critical decisions that result in an effective counterinsurgency campaign.

C. PURPOSE STATEMENT

The purpose of this research is to explore the application of network centric operations through the integration of hastily formed networks (HFN) and emerging technologies, which will be the foundation of a counterinsurgency model to assist the Royal Thai Armed Forces (RTARF) in resolving the insurgency problem in Thailand's southern regions. This technological framework will provide mission planners and military leaders with enhanced intelligence capabilities for data collection, access, analysis, decision support and collaboration as well as long-term information management (IM) to maintain information and decision superiority against the enemy.

D. PLAN FOR THE THESIS

This thesis aims to provide background about the current insurgent movement in southern Thailand, its history, and the political factors behind the Malay-Muslim rebellion. It explores the trends as well as the actors of the recent violence.

Discussion of the evolving nature of the insurgency and trends from 2004 to the present is also critical in understanding the dynamics of the problem, as it establishes an understanding of evolving insurgent tactics and violence. Having an awareness of the level of operational sophistication that the current insurgents have in their operations is a critical element in formulating a technological framework that undermines insurgent capabilities.

Thailand's southern separatist problem has resurfaced after a two-decade hiatus. For several decades, since the Cold War insurgency operations through recent struggles with drug and human trafficking, concerns about Thailand's porous border has been one of the Royal Thai government's top national security objectives. Understanding the "openness" of its borders, the RTARF has asked NPS to assist them in designing a concept of operations that incorporates the use of meshed networks, unmanned surveillance systems, and analytic tools to provide RTARF military leaders with superior information and decision support.

An analysis of the current RTARF counterinsurgency response, with regard to its operational effectiveness, and an assessment of the current security situation within the southern border provinces are provided. This research concludes by providing recommendations that the RTARF can use as a framework for integrating technology into their military operations.

We feel strongly that the current revolution in military affairs (RMA) is based on information. The need for information has created systems and concepts of warfare based on obtaining and distributing accurate information—fast. While information distribution is essential, another critical element is information analysis that leads to decision-making conducive to the disruption of enemy operations. The research paper seeks a technological solution that will provide the RTARF an edge in counterinsurgency warfare today.

The RTARF also has an emerging technology research and development program with specific emphasis on unmanned systems, and prototypes were demonstrated during the U.S.-Thailand Crimson Viper exercise in August 1–9, 2013. This paper will explore how these RTARF systems can be effectively integrated and operated through the ad hoc wireless mesh network and effectively conduct surveillance and feed information into a common operational picture tool.

Removing ambiguity— Carl von Clausewitz's explanation of the "fog and friction of war"—is the next great military challenge. Removing the ambiguity of who, what, where and when is the focus of this quest for information technology. Network centric operations are the new path to warfare. It is a force multiplier being heralded as the best,

non-nuclear, way to defeat an adversary. The concept has been embraced by the United States military in various ways in an effort to achieve the best solution for their operations; we see the same framework for the Royal Thai Armed Forces: the use of superior knowledge to exploit enemy weakness and concentrate military resources. Improvements in the RTARF's ability to decisively influence events in its southern border region will be the key to ending the Malay-Muslim insurgency problem that has caused disruption and instability in the country.

E. RESEARCH HYPOTHESES AND QUESTIONS

1. Research Hypotheses

- Hastily formed networks can provide the Royal Thai Armed Forces with a high level of situational awareness and execution across the battle space.
- The cumulative impact of superior information and decision making provides the RTARF with the capability to destroy the southern insurgency movement

2. Research Questions

- How effective is HFN technology in assisting the RTARF in its counterinsurgency (COIN) operations in southern Thailand?
- How does physical terrain and rural isolation in southern Thailand impact the effective employment and operation of an HFN wireless mesh?
- How does NPS' Lighthouse application assist the RTARF in counter-improvised explosive device (C-IED) and village stability operations (VSO)?
- What are the limiting factors in the range of the HFN mesh network? What methods can be employed and features implemented to extend the range?
- How does the RTARF resolve the logistical issues of supplying power to its equipment? How can operations be sustained without relying on fossil-fuel generators?
- How can HFN, Lighthouse and UAVs be integrated into a common operational picture?

F. RESEARCH METHODOLOGY AND SOURCES

Using a combination of primary and secondary sources, this thesis will provide an analysis of the Malay-Muslim insurgency problem in southern Thailand. A review of

previous academic research, industry white papers, technical journals, after action reports and vendor manuals will be conducted. Lessons learned during Crimson Viper 2013 in Hat Yao, Thailand, which allowed us the opportunity for field-testing and evaluation of proposed technologies, will be incorporated in this research. Crimson Viper 2013 was a technology demonstration sponsored by the MarForPac Experimentation Center (MEC) in collaboration with the RTARF, NPS Hastily Formed Networks Center and NPS Common Operational Research (CORE) Lab.

G. CHAPTER BY CHAPTER OVERVIEW

Chapter II: Analysis of the Current Security Situation: This chapter discusses the history of Thailand's southernmost provinces, the actors, trends in violence, the Thai government's response, and an analysis of the RTARF's military response.

Chapter III: Network Centric Warfare. This chapter covers concepts related to network centric warfare as an emerging theory of war and how it enables information superiority.

Chapter IV: Hastily Formed Networks. This chapter focuses on the concepts of hastily formed networks, ad hoc networking and the components that form an HFN wireless mesh during the Crimson Viper technology demonstration conducted in Hat Yao, Thailand, from August 1–9, 2013. This chapter also includes a discussion on the use of renewable energy to power HFN equipment as well as an overview of the Lighthouse application developed at the NPS' CORE Lab. It provides a background of the analytical methods used in developing Lighthouse as an effective analysis and common operational picture tool for commanders in understanding the battlespace as well as its application to military operations.

Chapter V: Conclusion: This section summarizes the work accomplished in this thesis and offers proposals for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ANALYSIS OF THE CURRENT SECURITY SITUATION IN SOUTHERN THAILAND

A. HISTORICAL BACKGROUND

There are approximately 2.8 million Thai-Muslims based on the official census conducted in 2000. The vast majority of the Thai population is Buddhist, while Thai-Muslims represent just 4.5% of the population (Maisonti, 2004, p. 6). Around eighty percent of Thailand's Muslim population lives in the southernmost provinces of Narathiwat, Pattani, Songkhla and Yala. There is a distinct difference between the mainstream Thai population and the population of these southernmost provinces, and the differences are based primarily on ethnic background, religious practices and language (Ampunan, 2007, p. 1). Ethnic Malays, in particular, have a considerable influence on Thai-Muslims because of their cultural and geographic affinity with Malaysia, (Maisonti, 2004, p. 6). In fact, there is a perception common throughout the country that Muslim Thais in the South would rather not be Thai and consider themselves as "Pattani Malays" (Janchitfah, 2005, p. 101).

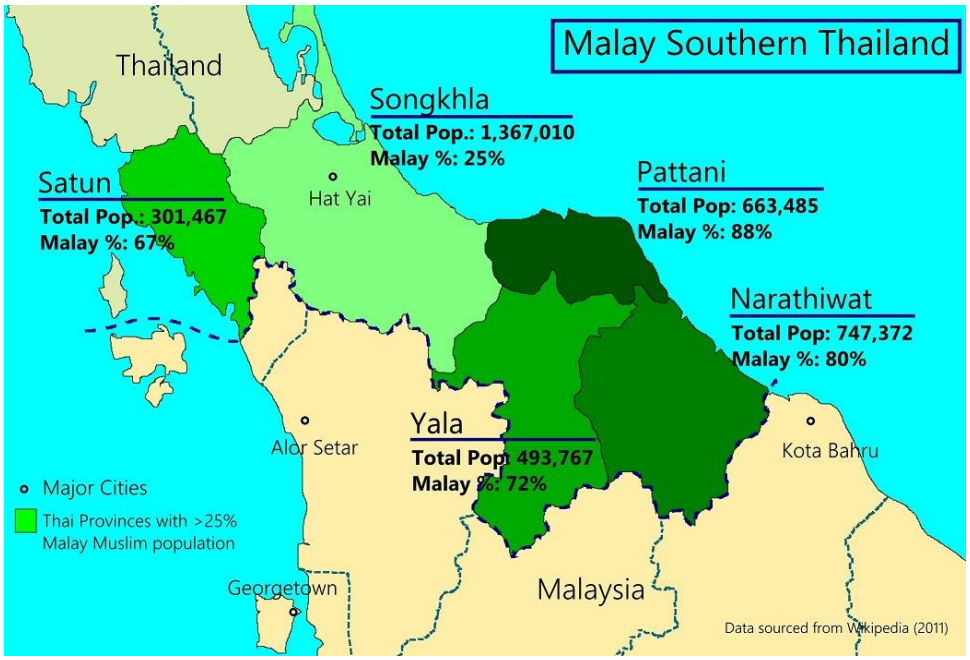

Figure 1. Map of Southern Thailand Showing Population Distribution (from Mkenology, 2012)

Lungasuka was the former name of what was known as the Kingdom of Pattani, and its territory included both Pattani province and Kedah province in Malaysia (Ampunan, 2007, p. 4). Today, this area is composed of the southernmost provinces of Thailand—Pattani, Yala and Narathiwat. Around the 15th and 18th centuries, the kingdom was also known as Pattani Darussalam and was acknowledged across the Malay world not only as a Malay Kingdom but as an Islamic Polity, or Dar Al-Islam. During that time, it was a center of commerce and trade for Southeast Asia as well as a major learning center for Islam, with most Islamic scholars describing it as the cradle of the Islamic religion in Asia (McCargo, 2008, p. 52). As a result, religions such as Hinduism and Buddhism saw a decline in followers while Islam expanded in the region, causing a shift to Islamic norms and traditions (Ampunan, 2007, p. 4).

The emergence of the Thai Chakkri dynasty in the 18th century changed the dynamics in the region as it sought to extend its influence and control over the Pattani kingdom. There was initial resistance from the Pattani people, but ultimately, the Siamese occupiers prevailed and expanded their control over the Pattani territories. As part of its occupation, the Chakkri dynasty also sought to eradicate the Pattani legal system, which conformed to Islamic law, and replace it with the Thai legal system, which was oriented toward Bangkok (Chalk, 2008, p. 2).

The 1930s marked the acceleration of the Thai government's efforts to assimilate the conquered Pattani region by carving out the region into three separate provinces—Narathiwat, Pattani and Yala, which were overseen by the Interior Ministry. As part of the assimilation process, the government embarked on a modernization program, which sought to eliminate all Malay dialects, local customs, Islamic traditions and adherence to shari'a law. The main purpose of this policy was to force the Malay-Muslims in southern Thailand to adopt the same social behavior and language as with the Thai majority (Chalk, 2008, p. 2).

In 1947 a more drastic policy known as "Thaization" was instituted. The proponents of this policy were generally authoritarian elements of the Thai military who successfully wrestled political power away from the civilian government. Thaization was a broad-based policy aimed at destroying the ethnic Malay identity and religious

affiliation with Islam. The policy also sought to further resist any autonomy in the southern provinces and force the population to adopt a Bangkok-friendly identity (Chalk, 2008, p. 4).

B. SOUTHERN RESENTMENT

As in most secessionist movements, the population's resentment emanates from a number of factors to include high incidence of poverty and lack of attention from the central government. This certainly applies to the southern provinces of Thailand, which continually suffer from high unemployment rates, and lack of government support ranging from basic infrastructure to education. Most of the grievances are based on these socio-economic factors that are exacerbated by cultural and religious incompatibility with the rest of Thailand (McCargo, 2010, p. 5).

Another source of resentment is the continued failure of the central Thai government to provide the Malay Muslim population with fair representation in matters that affect regional and national issues. There is a perceived injustice by the Malay population of the central government's tepid response in accommodating Malay-Muslims into the political process (ICG, 2007, p. 10).

The 1980s through the 1990s saw a reduction in insurgency driven violence, and this was in large part due to government efforts to include the Malay Muslims in the overall Thai political system. The Thai government promised changes in the southern region's socio-economic programs as well as improved security. However, most of the participants were Malay elites who did not necessarily represent the grievances of the majority concerning education, language and religious freedom and as such, a continued sense of discrimination continued to overshadow the region (McCargo, 2008, p. 7).

The conflict and levels of violence in southern Thailand saw an upswing during the administration of Prime Minister Thaksin Shinawatra. According to a 2011 report, *Conflict and Displacement in Southern Thailand* by the Internal Displacement Monitoring Center, "levels of violence started increasing in 2001 and in 2002, the dissolution by prime minister Thaksin Shinawatra of conflict-management bodies such as the Southern Border Provinces Administrative Centre (SBPAC) and the joint civilian-

police-military task force (CPM) weakened the government's capacity to deal with separatist tensions, and 119 insurgency-driven incidents were recorded in 2003" (Kok, 2011, p. 3).

The Thaksin administration adopted a strategy of increased military and police presence in the southern provinces, which also coincided with an anti-drug campaign that resulted in the deaths of almost 2,600 civilians (Chalk, 2008, p. 15). The civilian deaths were believed to be extra-judicial killings perpetuated by police forces, which also engaged in numerous human rights violations. There were also "blacklists" that targeted specific individuals, which roused more resentment and fear among the people (Kok, 2011).

In response to the targeted killings and abuses by police forces, a surge in insurgent-led violence occurred, culminating in an attack on a Royal Thai Army (RTA) base in the province of Narathiwat. The escalation of violence forced thousands of Malay-Muslims to leave the conflict areas creating a humanitarian crisis for the central Thai government. As a result, the Thaksin administration imposed martial law in 2004 followed by an emergency decree in 2005 that was in effect until 2011.

The implementation of martial law in the southern border provinces, created more widespread resentment among the Malays because of the human rights abuses that were committed by security officials and personnel and the blanket immunity that the government afforded them (ICG, 2007, p. 1). Human rights violations were prevalent, particularly against insurgent sympathizers and militants (HRW, 2007). Cases of torture and forced disappearances were widely reported. Several high-profile incidents such as the Tak Bai killing, Furquan and Krue Se Mosque attacks hasten the insurgent movement's resurgence beginning in 2004 (ICG, 2007, p. 5). The perpetrators of these attacks were never prosecuted, and the failure of the Thaksin government to hold the culprits accountable served only to reinforce the prevailing negative sentiment among the Malays of injustice and alienation (ICG, 2008, p. 2).

C. TRENDS IN VIOLENCE

For the first six years of the insurgency, most of the activity focused on low-intensity operations conducted by small groups of militants that targeted mainly off-duty security personnel, Buddhists, informants and community leaders cooperating with local authorities. Attacks were mainly assassinations and harassment. However, the start of 2009 marked the beginning of the insurgency's employment of improvised explosive devices (IEDs) focused initially on small-scale attacks on RTARF bases (JIR, 2013, p. 15). The introduction of IEDs into insurgent tactics resulted in a gradual increase in casualties.

According to data compiled by Zachary Abuza in *The Ongoing Insurgency in Southern Thailand: Trends in Violence, Counterinsurgency Operations and the Impact of National Politics*, "between December 2008 and June 2011, 949 people were killed and more than 1,700 wounded, which represented a monthly average of 32 and 58, respectively" (Abuza, 2011). The numbers are illustrated in Table 1, showing a spike in the number of people killed and wounded during that period.

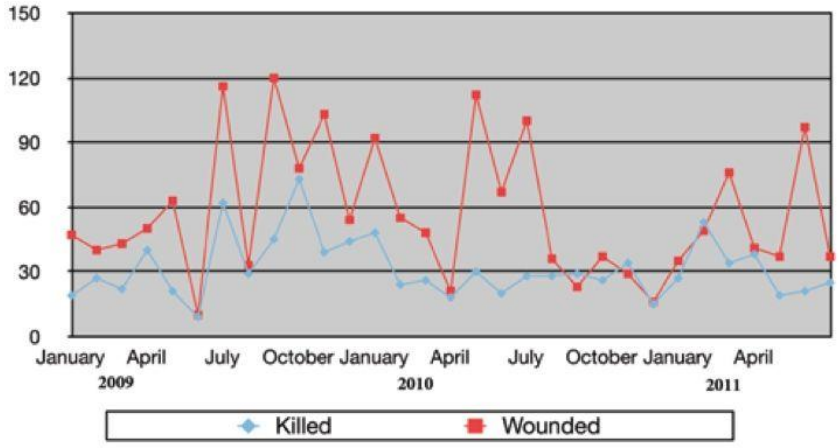

Table 1. 2009–2011 Casualties (from Abuza, 2011)

Based on the same 2011 study, the casualties inflicted on RTARF security forces were mainly from insurgent IED attacks. These attacks were carried out mostly in remote villages while RTARF forces conduct escort missions to protect teachers and Buddhist

monks (Abuza, 2011, p. 6). However, despite the large number of wounded security personnel, there were fewer troop fatalities, which represented only 20 percent of the total casualty count.

Local police forces suffered casualties, as well, because of their presence in the countryside, mainly augmenting the RTARF security detail. A total of 44 police personnel were killed and 214 were wounded from 2009 to 2011 (Abuza, 2011, p. 7).

Complementing the RTARF and police forces were village defense volunteers (VDVs) and rangers. VDVs were particularly vulnerable to insurgent attacks as they were normally ill-equipped volunteers from the surrounding villages who were lightly armed. On the other hand, the rangers were predominantly migrants from northern Thailand, which the RTARF organized into a paramilitary group. However, the rangers were poorly trained and were utilized by the RTARF as an augmenting force in the rural areas (Abuza, 2011, p. 7) Casualty numbers for both rangers and VDVs include 122 killed and 185 wounded, mostly from IED attacks while conducting teacher protection duties.

Civilians made up most of the casualties as represented in figures 2 and 3. The total number of civilian deaths for the period of 2009 to 2011 was 594; 902 civilians were wounded (Abuza, 2011, p. 7). The high proportion of civilian casualties was due to targeted attacks by the insurgents on Buddhist civilians. Buddhist civilians were natural targets as they were widely viewed by Malays as symbolic representatives of the central Thai government. The insurgents also targeted Muslim civilians who were suspected of collaborating with the Thai authorities. IED attacks occurred mostly in public areas which resulted in heavy civilian casualties (McCargo, 2008, p. 4).

From 2009 to 2011, insurgent attacks were less random compared to the earlier years of the insurgency and a retaliatory pattern evolved in response to actions by the RTARF security forces. Consequently, civilians suffered the most in terms of casualties as a result of these insurgent attacks (Abuza, 2011, p. 5).

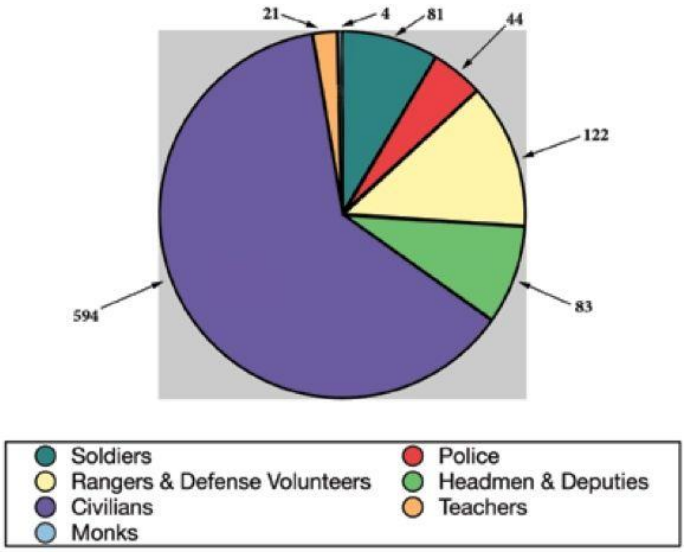

Figure 2. Number Killed (by Category), 2009–2011 (from Abuza, 2011)

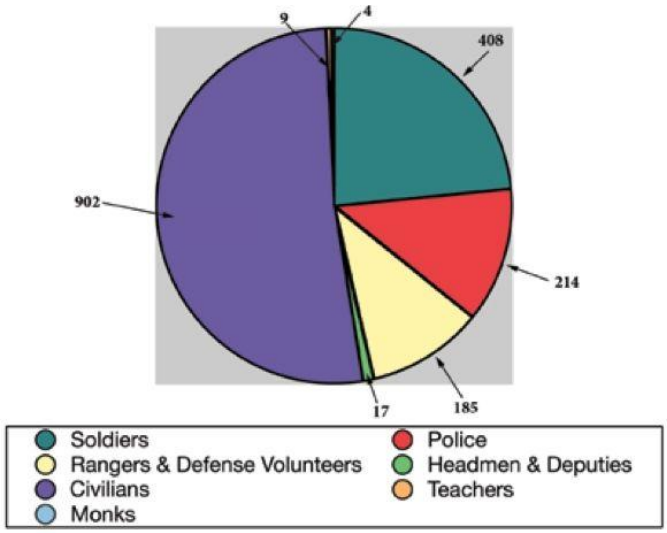

Figure 3. Number Wounded (by Category), 2009–2011 (from Abuza, 2011)

The years 2011 to 2012 saw a sharp rise in IED attacks and an increased level of sophistication and scale of insurgent operations. This included nine large blasts using car bombs and IEDs. One large car bomb was directed toward an entire block of apartment buildings occupied by police forces, and another attack targeted 12 shop houses, both of which wounded a total of 18 people. The IEDs deployed by insurgents have also

increased in size and complexity from an average of 5 to 10 kilograms to 15, sometimes exceeding 20 kilograms. The use of larger IEDs by the insurgents has become an emerging trend, as three out of the 12 IED attacks in 2011 were 15 kilograms or more (Abuza, 2011, p. 8).

According to a 2013 report from *Jane's Intelligence Review*, there was also an increase in the number of professionally executed ambushes or drive-by attacks involving insurgents operating in section strength and often with several vehicles (JIR, 2013, p. 15). Most ambushes were better coordinated and involved the use of large IEDs or vehicle-borne improvised explosive devices (VBIEDs) against RTARF convoys by well-armed insurgents.

Major assaults on RTARF bases were also undertaken by the insurgent fighters, often dressed in military fatigues, who appeared to be professionally trained and well-equipped. Insurgent operations involved semi-regular units operating at platoon and half-company strength, showing an increased level of organization. These attacks were aimed primarily at seizing weapons, occurring mostly in the strategically central zone of Narathiwat province (JIR, 2013, p.15).

Since 2012 insurgents continue to employ IEDs with their operations; however, an expansion of insurgent operations into urban areas has evolved. On the weekend of February 16–17, 2013, a series of IED and incendiary attacks occurred in Pattani City, and large-scale IED attacks hit Narathiwat and Yala provinces (JIR, 2013, p. 16). These attacks were considered a response to a failed assault by insurgent forces on an RTARF base in Narathiwat province, which resulted in the deaths of 16 insurgent members by RTARF security forces. Although this particular attack was a significant setback to insurgent operations, particularly in Narathiwat, the attack underscores the evolving nature of the insurgency and the increased sophistication and growth of the movement.

D. INSURGENTS

The Barisan Revolusi Nasional Coordinate (BRN-C) has been identified by the RTARF as the main organizational driver behind the current insurgency in southern Thailand (JIR, 2013, p. 14). It is a loose network of separatist militants, broadly shaped

by Maoist theories of revolutionary people's war. Based on a 2013 report by *Jane's Intelligence Review*, the BRN-C's Maoist model of popular mobilization had involved the setting up of clandestine, village-level political committees, which direct economic, fund-raising and logistical activities. This model has also organized civilians into functional groups for youth, women and Islamic clerics, which gives the BRN-C a base of support that allows the movement to fulfill intelligence gathering, military recruitment and covert operations (JIR, 2013, p. 14).

According to a 2011 report by the Human Rights Watch (HRW), "the BRN-C may have up to 3,000 fighters and around 40,000 supporters" (HRW, 2011, p. 2). The BRN-C does not recognize the Thai constitution and political system and from the time of its inception, it committed itself to armed struggle. The organization's goal is to create a sovereign state composed of the southern Muslim provinces (Chalk, 2008, p. 5).

The BRN-C operates in relative secrecy and not much is known about its leaders and organizational planning. Although it is believed that the group follows a pyramid-shaped structure along classic Maoist lines, with the base of that structure consisting of an unarmed militia, involving women, elderly citizens and sometimes children. The BRN-C uses this element to support its intelligence-gathering and logistical activities, particularly in moving weapons from its base of operations to attack sites. Additionally, the BRN-C has orchestrated noisy demonstrations against RTARF forces in the southern provinces, with participants coming mostly from this support base. Furthermore, youth groups were deployed to conduct vandalism and other nefarious activities across the southern districts to underscore the BRN-Cs ability to coordinate operations. The process also serves as an indoctrination for youth interested in joining the movement. At the middle of that pyramid is the bulk of its armed force that are locally organized into small patrol groups consisting of six to seven fighters, that can be expanded upwards to form company size units (JIR, 2013, p. 15). At the top of the pyramid are commando units, command and control elements and its top leadership who possess advanced training and specialized skills such as demolition, close-quarter assault and combat medicine. This group has been blamed for most of the recent IED attacks and coordinated assaults on RTARF bases, including the January 2004 raid on an army camp which sparked the

beginning of the current insurgency. Since then, a total of eight assaults have taken place, mostly in the strategically central province of Narathiwat.

E. THAI GOVERNMENT RESPONSE

In September 2006, the Thai government established the Internal Security Operations Command (ISOC) based on the 2007 Internal Security Act signed by Prime Minister Surayud Julanont, former general in the Thai Special Forces who took over the government in a bloodless coup. The ISOC has four units:

(1) Civil-Police-Military (CPM) 43

(2) Southern Border Provinces Administrative Charter (SBPAC)

(3) Southern Border Provinces Peace-Building Command (SBPPC)

(4) Police Special Task Force

CPM 43 is the ISOC's military wing while the SBPAC serves as the socio-economic wing. This unit is also tasked with executing the government's peace and reconciliation efforts and management of security forces. The SBPPC on the other hand serves as the joint intelligence center that coordinates all intelligence units and activities at all levels. Lastly, the Police Special Task Force is the unit responsible for the investigation and arrest of suspects (Ampunan, 2007, p. 16)

The ISOC is the RTARF's main organizing body that manages the government's security agenda and strategy as well as the implementation of critical projects in southern Thailand.

2. Force Composition

According to a 2008 research by the *National Defense Research Institute*, "CPM 43 deployed 18,000 police officers; 30,000 military troops from all parts of Thailand; and 18,000 local volunteers from the ministry of the interior, including 4,000 local soldiers from the 15th Light Infantry Division, widely dispersed over the southern Thailand provinces" (Chalk, 2008, p. 107).

Deployed RTARF forces numbered at 66,000, or roughly the equivalent of 21 battalions. These troops were deployed to a mostly rural area that covers approximately

70,713 square kilometers. These troops were deployed to provide security, village stabilization operations, protection detail for Buddhist monks and teachers and overall restoration of law and order. The RTARF force, were also augmented by 7,500 VDV paramilitary troops that were recruited locally to provide border security, supplement intelligence-gathering activities and act as a light screening forces (Rodthong, 2009, p. 22). These paramilitary forces have a distinct advantage in that they use the same local language and understand local culture.

The southern deployment of the RTARF force called for a normal rotation of six months, and was relieved by fresh units from the north at the conclusion of the deployment period. However, deployments were extended for periods greater than six months, and troops were continuously redeployed to the same areas after serving their initial tours.

The increased troop presence and regularity of deployments has seen mixed results. According to the 2009 report, *Southern Crisis and Daily Violence,* "while the number of violent incidents was statistically reduced, the number of deaths and injuries has increased" (Matichon, 2009). This can be attributed to the increasing levels of sophistication of the insurgent groups and their employment of increasingly lethal IEDs as their weapon of choice (Rodthong, 2009, p. 23).

3. Intelligence Activities

According to the 2007 study, *The Need for Intelligence Reform in Thailand's Counterinsurgency*, there are multiple intelligence elements within the ISOC structure:

(1) ISOC Intelligence
(2) Situation Monitoring Division
(3) 4th Internal Security Operations Region
(4) 4th ISOR Intelligence Coordinating Center
(5) CPM43 Joint Intelligence Center

The RTARF controls the activities of ISOC Intelligence, which acts as the central hub for all intelligence analysis. On the other hand, the Situation Monitoring Division falls under the guidance of the Internal Security Coordinating Center (ISCC) within the

ISOC and is responsible for monitoring developing situations and follow-on action. These two intelligence elements have duplicative functions and there is mostly confusion between their staffs with regard to delineation of intelligence responsibilities since their missions are similar (Ampunan, 2007, p. 31).

Intelligence operations continue to rely mainly on human intelligence (HUMINT), which is mostly unreliable given the BRN-C's penetration of most villages and the popular support it has in the southern provinces. This heavy reliance on HUMINT does not provide the RTARF with critical information to make an immediate and effective impact in its military operations.

The same 2007 study also explains the current intelligence structure, which is extracted as follows:

> The intelligence element of the 4th Internal Security Operations Region (ISOR) is subordinated to only the military to integrate the intelligence tasks. For intelligence operations, there is the 4th ISOR Intelligence Coordinating Center that is responsible for intelligence operation, but it is assigned under operational control of the CPM43 Joint Intelligence Center. The CPM43 is the subordinate unit of the 4th ISOR but it controls the operation of the 4th Intelligence Coordinating Center. The reason for this kind of command structure, assigned at the order of the Office of Prime Minister, is to increase the effectiveness of intelligence cooperation and operation for CPM43 in rapidly pursuing the situation. However, this management structure creates an overlap in the chain of command and decreases the unity of the command. (Ampunan, 2007, p. 32)

Essentially, there is no unity of effort that produces a common operational picture (COP) for Thai government policy makers and RTARF commanders as competing interests and parallel tasks exist within a convoluted intelligence structure.

4. Government Peace Efforts

There was consensus that the heavy-handed policies implemented by the Thaksin administration, which relied extensively on the police to carry out counter-insurgency operations, violated human rights and worsened the violence in the south (Arugay, 2012, p.16).

Prime Minister Julanont issued an apology in October 2006 to atone for the policies and injustices carried out by the Thaksin administration. It was an attempt by the new government to reach out to the insurgents for negotiations and inclusion into the political process. An amnesty program was proposed along with the cancellation of rebel blacklists that the previous government used to pursue insurgent leaders (Klaimanee, 2008, p. 79).

Despite this effort, no formal agreements were made, and majority of Muslim-Malays viewed the government outreach with suspicion, given Julanont's background as a former military general (Rodthong, 2009, p. 23).

More recently, the Thai government and separatist representatives signed an accord in Kuala Lumpur, Malaysia on February 28, 2013, which committed both parties to begin a formal dialogue process, to be facilitated by Malaysia (JIR, 2013, p. 14). However, violence has continued in southern Thailand and a deep-seated mutual distrust continues to exist between both parties, which suggest that a peace settlement remains out of reach.

F. SUMMARY

The issues faced by the RTARF in southern Thailand not only involve security, but a complex web of socio-economic, political and administrative issues unique to the Malay-Muslim problem. The current conflict lacks the elements of a conventional war and yet the RTARF is slow to recognize this fact and continues to approach the problem with conventional military strategy. Our research suggests that the current conflict has all the elements of irregular warfare, which necessitates a new concept of operations, particularly in the areas of intelligence gathering and information sharing.

The statements below were extracted from a personal interview with Senior Colonel Sorakoset Piamyart, and Colonel Jaturong Juntaranont, by Tibordee Ampunan in June 21, 2007, which support our suggestion for a fundamental change in the RTARF's concept of operations that favors a technology driven framework that supports sophisticated intelligence analysis, data collection and real-time information sharing.

> The RTARF's intelligence organizations put emphasis on collection rather than analysis, so that most of the intelligence reporting is somewhat scattered and accumulated at the analysis section without sufficient integration to create an entire picture of what would be useful in eliminating the insurgent organizations.
>
> In the case of the responsible government organization, it must re-adjust its structure and administration in order to improve and allow all agencies to access information both faster and simultaneously as a network—not a hierarchy—and facilitate access among all levels. This does not mean transforming the bureaucracy into a network, but it means applying the benefit of networks that are embedded in hierarchical organizations to increase the speed and efficiency for cooperation and the sharing of information. Therefore, the establishment of an information center may alleviate this limitation through the use of information technology, which would not only store and arrange the information, but determine who can access it. Information technology will enhance the capability of the network by allowing all agencies to coordinate efforts and exchange and disseminate information in real time. (Ampunan, 2007, p. 33)

Establishment of an information center can be achieved through a framework that leverages the use of hastily formed networks (HFN). HFN technology provides a low cost approach that helps address this information technology gap. Using commercial off the shelf (COTS) components that are detailed in chapter four, HFN technology helps provide coordination and unity of effort through a wireless communications infrastructure that allows data storage, sharing, and real-time access to critical information that is required for the Thai government's operations in southern Thailand. With an HFN wireless communications backbone, the government can also fully harness the power of NPS' Lighthouse technology that allows rapid mobile data collection and sharing using tablets and smartphones as well as social network and geospatial analysis, providing enhanced common operational picture capability, for a multi-agency structure.

This new technology framework is critical, especially for the RTARF's C-IED and VSO activities, as it provides them with enhance analytical capabilities that overcomes the weaknesses of their current intelligence collection and analysis model. Social networking in particular provides a powerful insight into understanding the human terrain. With resurging militant groups such as the BRN-C who gain strength through popular mobilization and clandestine activities at the village-level, HFN technology as

the network layer integrated with Lighthouse technology on the application layer, provide the RTARF with information superiority that allows them to be a step ahead of the adversary.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK CENTRIC WARFARE

> *What we are seeing, in moving from the Industrial Age to the Information Age, is what amounts to a new theory of war: power comes from a different place, it is used in different ways, it achieves different effects than it did before. During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed. We have come to call that new theory of war network centric warfare. It is not only about networks, but also about how wars are fought—how power is developed.*
>
> —Vice Admiral (Ret.) Arthur K. Cebrowski,
> director of Office of Force Transformation

A. THE WAY AHEAD

In order to transition from the RTARF's dominant and more traditional state of troop-based kinetic warfare into a more decentralized multi-agency effort, a new way of executing conflict management must be considered. The high-OPTEMPO nature of the RTARF's counter-insurgency efforts requires a hardware footprint that allows for rapid deployment of communication infrastructure, coupled with a well-developed doctrine of information management as it applies to war. Understanding this doctrine, Network Centric Warfare, is key to the development of a force that can use modern communications systems to gain a critical advantage.

B. BACKGROUND

In recent years, military leaders, particularly in the United States, have looked increasingly at using networks to reduce response time and increase the speed of decision-making during operations. The ever-evolving nature of warfare and the employment of non-conventional, asymmetric tactics by non-state actors now require a different approach.

Countering asymmetrical threats as they relate to a country's internal security requires the ability to perform various roles with high speed, small size, and reliable technology. These asymmetrical threats potentially challenge traditional command and control (C2) structures. Therefore, emerging technologies, such as UAVs, ground sensing

and mobile data collection devices all linked via wireless networks, present increased capability for security forces deployed to remote areas of operation and also help to facilitate shared situational awareness across the combat spectrum.

Network Centric Warfare (NCW) is the military's solution to the problem of how to adapt warfare to the Information Age. The availability of information, the speed with which it may be accessed, and the ability to rapidly disseminate it have become increasingly vital to maintaining a favorable balance of power on the battlefield. The nearly continuous flow of information in modern warfare has allowed NCW to become an entirely new way of planning and executing missions. NCW generates increased combat power for geographically dispersed forces by linking kinetic assets, sensor data, and personnel "to achieve shared intelligence, battlespace awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization in support of mission accomplishment and an end result wherein the whole is greater than the sum of its parts" (Alberts, 2000, p.65).

For the RTARF, this creates a situation where its forces are able to achieve a high degree of operational maneuver and speed of movement without requiring the amassment of assets traditionally associated with victory in the past. With increased speed and improved synchronization, the impact to operations in everything, from support areas through combat zones, is immediate. The violence in southern Thailand, which is one form of asymmetrical warfare, along with terrorism, are all recognized as major threats to its security and stability.

In early 2005, the Commander-in-Chief (CINC), Royal Thai Air Force (RTAF), published two documents that indicated the RTAF's and the Royal Thai government's vision for the future. Their desires are to develop a military that is more capable, leaner, and embraces technology. The first document, "RTAF's Operational Policy for Budget Year 2548," in the area of Operations Policy, CINC/RTAF calls for the RTAF to, "6.4.5 develop command and control capabilities by digitizing their system for command and control so that future requirements and developments can embrace technological advances which will move towards a network centric capability." CINC/RTAF further discusses how the RTAF should "work with allied nations on R&D" and how "R&D

should match RTAF needs" (Valentine, 2005, p. 51). These documents illustrate that the RTARF recognizes the need for a technological framework to support its military operations into the future and allies such as the United States can assist in its goal of achieving a highly networked force.

C. INFORMATION SUPERIORITY

Information superiority, according to the U.S. Department of Defense (DoD), *Joint Publication 1-02*, is defined as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition…providing the operational commander the ability to see and hear virtually anything of importance to his/her operation" (JP 1-02, 2005).

Achieving information superiority provides commanders an advantage, allowing them to accomplish their mission using superior control of information while simultaneously exploiting (or outright denying) the enemy's ability to do the same. Throughout history, information superiority has been regarded among military leaders as a cornerstone of military success. The famous Chinese military strategist Sun Tzu wrote in *The Art of War*

> He who has a thorough knowledge of his own conditions as well as the conditions of his enemy is sure to win in all battles. He who has a thorough knowledge of his conditions but not the conditions of the enemy has an even chance of winning and losing a battle. He who has neither a thorough knowledge of his own conditions nor the conditions of the enemy is sure to lose in every battle.

Information superiority is the fulcrum upon which military victory is balanced. There is no advantage to be gleaned from a lack of knowledge—this much remains true. What has changed, however, is that "many capability-enabling technologies in an information-driven era" have converged in recent decades. The simultaneous and synergistic emergence of new threat scenarios has solidified information superiority as an absolute necessity to achieving victory (JCS, 2010). Figure 4 is a graphical illustration extracted from the book *Network Centric Warfare: Developing and Leveraging Information Superiority*, which highlights how a superior information position, allows a force to dominate its adversary.

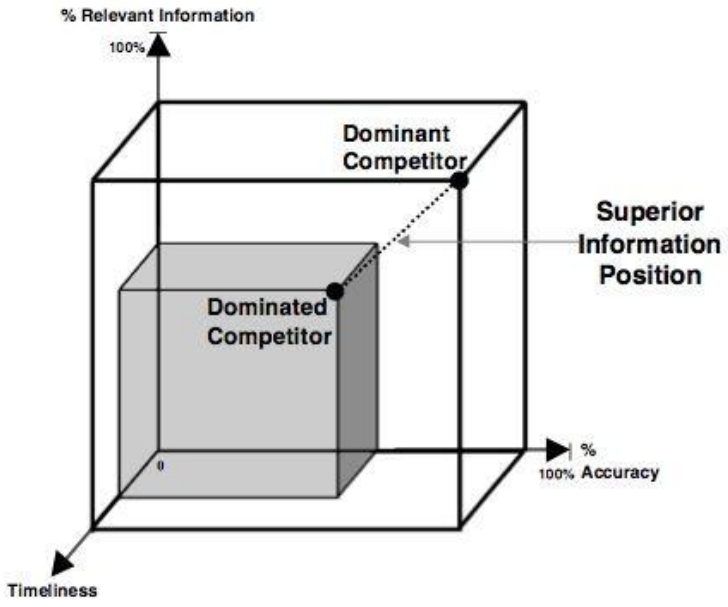

Figure 4. Superior Information Position (from Alberts, 2000)

Information superiority is a force multiplier for a commander. It allows for new options where none existed before; it improves the effectiveness of those options already available; it even allows a commander to preempt options seemingly available to an adversary. The result is rapid victory at a reduced cost. This frees resources to operate at a higher tempo and provides more opportunities to diminish the opportunities and advances an adversary may be seeking to exploit.

Carl von Clausewitz has famously articulated about the fog and friction of war. As a result of this enduring characteristic of war, centuries of military operations have focused on accommodating a lack of information; that is, how to deal with the fog of war. Fog pertains to uncertainty: "uncertainty about where everyone is, what their capabilities are, and the nature of their intentions." (Alberts, 2001, p.5) Until recently a commander could not even have a timely and accurate picture of his own forces let alone be comfortable about where the enemy was and what they were up to. Friction is about the glitches that occur in carrying out plans to synchronize forces or even to accomplish the simplest tasks. Some of this friction can be attributed to fog, poor communications, and lack of shared knowledge.

Decision-making in war carries with it an extremely high cost of error. Therefore, it is not surprising that military concepts of operation, organizations, doctrine, and training have always been preoccupied with reducing the effects and risks associated with fog and friction. However, advances in technology and network centric operations offer the opportunity to reduce fog and friction through better communications, synchronization of movement and knowledge sharing.

Table 2, which highlights the objective of information superiority, is extracted from the 2001 book, *Understanding Information Age Warfare* by David Alberts, director of the DoD's Research & Strategic Planning Office and one of the foremost experts on information superiority. The table illustrates the relationship between the amount of fog and friction and effectiveness.

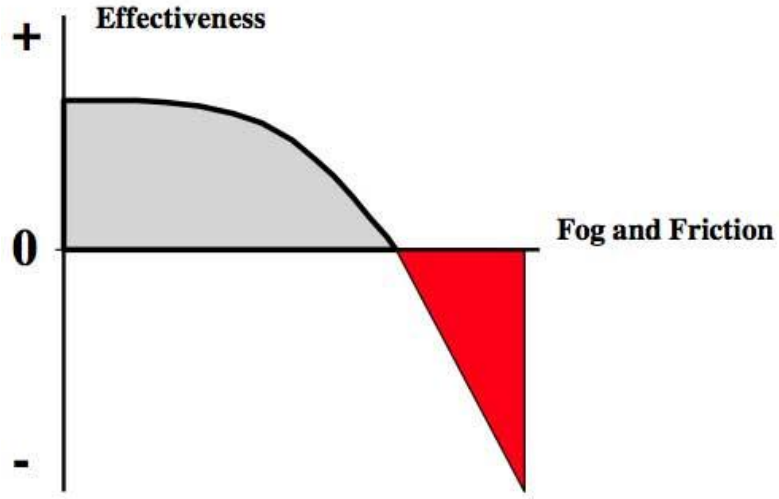

Figure 5. Objective of Information Superiority (from Alberts, 2001)

According to Alberts, the level of communication and synchronization directly correlates to effectiveness in military operations. The goal is to operate in various parts of the shaded area, and to avoid the lower right (red) area, which is fog and friction (Alberts, 2001, p. 5). Network centric operations enable military forces to consistently operate in the shaded areas by providing capabilities to better communicate, synchronize and share critical knowledge in the battlespace, and ultimately improve military effectiveness.

D. DOMAINS OF CONFLICT

Understanding the effect of information on a force's operational capabilities requires familiarity with four domains—the physical domain, the information domain, the human domain and the cognitive domain. Figure 5, illustrates graphically how these domains are integrated with each other.

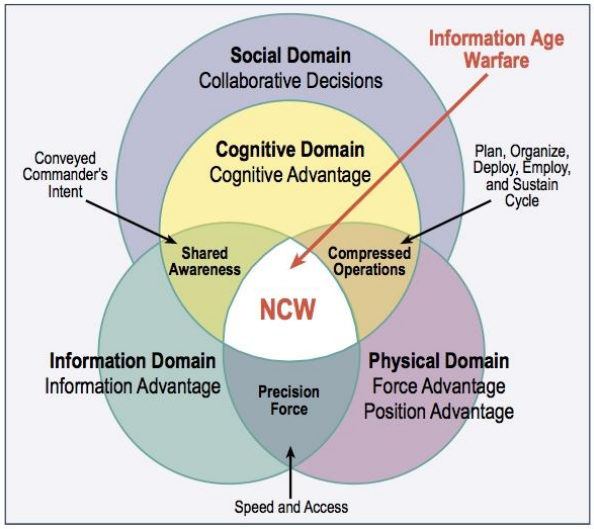

Figure 6. Network Centric Warfare and the Domains of Conflict (from U.S. DoD, Office of Force Transformation, 2002)

This concept was extracted from the *2005 DoD Manual on Implementation of Network Centric Warfare* and is presented in original form in Table 3 to preserve the integrity of the concepts discussed.

Table 2. DoD's Network Centric Warfare Domains (from DoD, 2005)

1. Physical Domain

The physical domain is the traditional domain of warfare where a force is moved through time and space. It spans the land, sea, air, and space environments where military forces execute the range of military operations and where the physical platforms and communications networks that connect them reside. Comparatively, the elements of this domain are the easiest to

measure and, consequently, combat power has traditionally been measured in the physical domain.

2. Information Domain

The information domain is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. This is the domain of sensors and the processes for sharing and accessing sensor products as well as "finished" intelligence. It is where C2 of military forces is communicated and the commander's intent is conveyed. Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions by an adversary.

3. Cognitive Domain

The cognitive domain is in the mind of the warfighter. This is the realm of effects based operations (EBO). Many, though not all, battles, campaigns, and wars are won in this domain. The intangibles of leadership, morale, unit cohesion, level of training and experience, and situational awareness are elements of this domain. This is the domain where commander's intent, doctrine, tactics, techniques, and procedures reside. This is also where decisive battlespace concepts and tactics emerge.

4. Social Domain

The social domain describes the necessary elements of any human enterprise. It is where humans interact, exchange information, form shared awareness and under- standings, and make collaborative decisions. This is also the domain of culture, the set of values, attitudes, and beliefs held and conveyed by leaders to the society, whether military or civil. It overlaps with the information and cognitive domains, but is distinct from both. Cognitive activities by their nature are individualistic; they occur in the minds of individuals. However, shared sense-making—the process of going from shared awareness to shared understanding to collaborative decision making—is a socio-cognitive activity because the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa.

E. PRINCIPLES OF NETWORK CENTRIC WARFARE

Within the same 2005 DoD manual, *Implementation of Network Centric Warfare* are nine governing principles underlying NCW. They are the core of NCW's continuously evolving "theory of war in the Information Age." These insights on NCW

principles have been extracted from the manual. Additionally, Figure 5 illustrates how NCW principles span the domains of conflict discussed in the previous section.

Table 3. DoD's Network Centric Warfare Principles (from DoD, 2005)

(1) Fight First for Information Superiority

- Generate an information advantage through better timeliness, accuracy, and relevance of information.
- Increase an enemy's information needs, reduce his ability to access information, and raise his uncertainty.
- Assure our own information access through a well networked and interoperable force and protection of our information systems, including sensor systems.
- Decrease our own information needs, especially in volume, by increasing our ability to exploit all of our collectors.

(2) Shared Awareness

- Routinely translate information and knowledge into the requisite level of common understanding and situational awareness across the spectrum of participants in joint and combined operations.
- Build a collaborative network of networks, populated and refreshed with quality intelligence and non-intelligence data, both raw and processed, to enable forces to build a shared awareness relevant to their needs.
- Information users must also become information suppliers, responsible for posting information without delay. Allow access to the data regardless of location.
- High-quality shared awareness requires secure and assured networks and information that can be defended.

(3) Speed of Command and Decision Making

- Recognize an information advantage and convert it into a competitive advantage by creating processes and procedures otherwise impossible (within prudent risk).

- Through battlefield innovation and adaptation, compress decision timelines to turn information advantage into decision superiority and decisive effects.
- Progressively lock out an adversary's options and ultimately achieve option dominance.

(4) Self-Synchronization

- Increase the opportunity for low-level forces to operate nearly autonomously and to re-task themselves through exploitation of shared awareness and the commander's intent.
- Increase the value of subordinate initiative to produce a meaningful increase in operational tempo and responsiveness.
- Assist in the execution of the "commander's intent." Exploit the advantages of a highly trained, professional force.
- Rapidly adapt when important developments occur in the battlespace and eliminate the step function character of traditional military operations.

(5) Dispersed Forces

- Move combat power from the linear battlespace to non-contiguous operations.
- Emphasize functional control vice physical occupation of the battlespace and generate effective combat power at the proper time and place.
- Be non-linear in both time and space, but achieve the requisite density of power on demand.
- Increase close coupling of intelligence, operations, and logistics to achieve precise effects and gain temporal advantage with dispersed forces.

(6) Demassification

- Move from an approach based on geographically contiguous massing of forces to one based upon achieving effects.
- Use information to achieve desired effects, limiting the need to mass physical forces within a specific geographical location.
- Increase the tempo and speed of movement throughout the battlespace to complicate an opponent's targeting problem.

(7) Deep Sensor Reach

- Expand uses of deployable, distributed, and networked sensors, both distant and proximate, that detect actionable information on items of interest at operationally relevant ranges to achieve decisive effects.
- Leverage increasingly persistent intelligence, surveillance, and reconnaissance (ISR).
- Use sensors as a maneuver element to gain and maintain information superiority.
- Exploit sensors as a deterrent when employed visibly as part of an overt display of intent.
- Enable every weapon platform to be a sensor, from the individual soldier to a satellite.

(8) Alter Initial Conditions at Higher Rates of Change

- Exploit the principles of high-quality shared awareness, dynamic self- synchronization, dispersed and de-massed forces, deep sensor reach, compressed operations and levels of war, and rapid speed of command to enable the joint force to swiftly identify, adapt to, and change an opponent's operating context to our advantage.
- Warfare is highly path-dependent; hence, the imperative to control the initial conditions. The close coupling in time of critical events has been shown historically to have profound impact both psychologically and in locking out potential responses.

(9) Compressed Operations and Levels of War

- Eliminate procedural boundaries between Services and within processes so that joint operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects.
- Increase the convergence in speed of deployment, speed of employment, and speed of sustainment.
- Eliminate the compartmentalization of processes (e.g., organize, deploy, employ, and sustain) and functional areas (e.g., operations, intelligence, and logistics).

- Eliminate structural boundaries to merge capabilities at the lowest possible organizational levels, e.g., joint operations at the company/sub-squadron/task unit level.

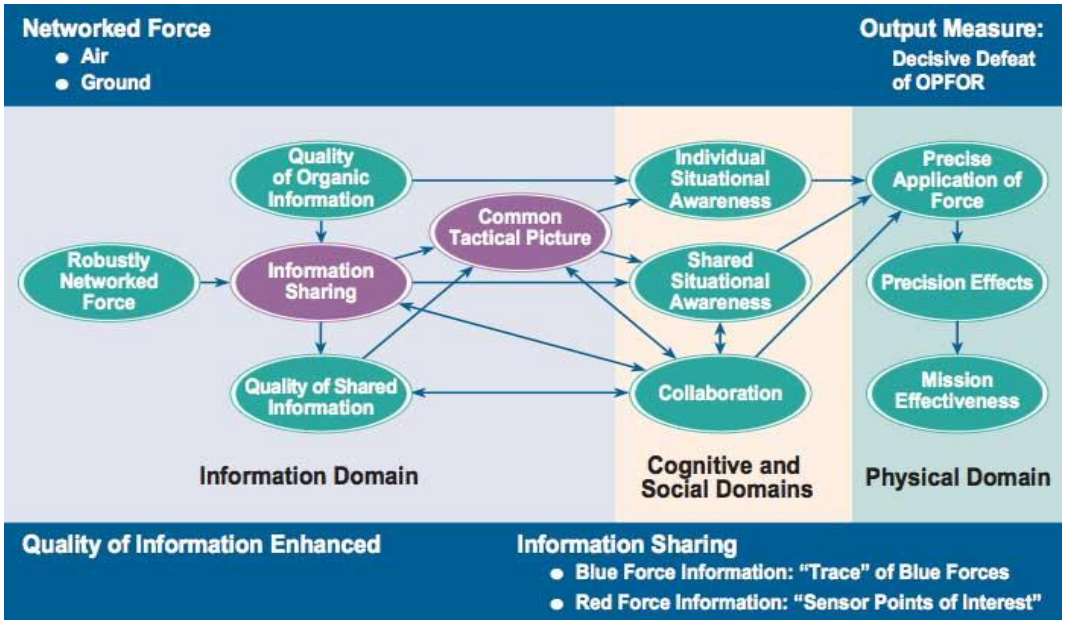

Figure 7. NCW Concept (from DoD, Office of Force Transformation, 2005)

F. SUMMARY

Network centric warfare is an emerging theory of war that is becoming an integral part of how most militaries are transforming. It takes information superiority and translates it into effective responses and actions. As a war fighting concept, it relies upon kinetic assets, sensor data, and personnel being thoroughly connected through rapid, networked communication channels in order to synchronize effort by sharing knowledge and awareness. Significantly increased combat power comes as a result of this achievement of improved awareness and the ability to share it, providing the means with which to operate at a higher tempo, expedite command execution, and streamline warfighter support. The result will be greater lethality and effectiveness, increased survivability, and reduced collateral damage and risk.

Although Network Centric Warfare is the framework for more effective use of advanced communications technology to more efficiently combat adversaries, developing

the proper communications infrastructure is of equal importance. The RTARF's operating environment and the high tempo nature of their counter-insurgency operations will require a networking concept that will be agile enough to meet their demands.

IV. HASTILY FORMED NETWORKS

Hastily formed networks is a networking concept that employs rapidly deployable wireless ad hoc networks that is sourced mainly from commercial of the shelf (COTS) hardware and open-source software technologies leveraging the 802.11 WiFi and 802.16 wireless standards. HFNs are designed to be self-contained and portable so they can be used to create nodes in remote areas where there is currently no electricity, and no network connectivity; they act as an extension of the enterprise network (see Figure 6).

The main purpose of HFN technology is to facilitate operations in austere environments, allow communications and interoperability between units and share operational information. Information sharing is a critical element for any mission as it provides military planners with a common operational picture that enhances their situational awareness and an in-depth understanding of operational needs. Without a robust communications infrastructure, command and control of highly mobile forces that are geographically dispersed would be difficult (Hwee, 2007, p. 3). Figure 7 represents the various pieces to the HFN puzzle, integrated to form a robust capability.

Figure 8. Hastily Formed Network Components (from Steckler, 2013)

The U.S. Naval Postgraduate School's Center for Hastily Formed Networks sent a team of students to participate in the Crimson Viper technology demonstration in Hat Yao, Thailand from August 1–9, 2013, to demonstrate HFN technology to the RTARF. The main objective was to create a wireless communications network to support participating units in and around the Hat Yao operating area using the wireless communication technologies that comprise a hastily formed network. Figure 8 provides a map of the wireless network footprint established in Hat Yao, Thailand for Crimson Viper 2013.

As demonstrated by the Naval Postgraduate School's Humanitarian Assistance/Disaster Relief (HA/DR) missions during the Asian tsunami in 2004, Hurricane Katrina in 2005 and the 2010 Haiti earthquake, HFN technology has proven to be an effective communications and networking platform. This is reported by the university's HFN research group's after action reports (AAR) found in appendix A of this thesis.

Crimson Viper 2013 was an opportunity to demonstrate to the RTARF that the same concepts applied to HA/DR can also be employed in a tactical military environment as part of a network centric approach that enhances command and control, facilitates real-time access to surveillance information and enables interoperable communications via voice/data/video communications in an area such as the insurgency plagued provinces of southern Thailand. A robust wireless network that can be sustained in austere field environments providing the products mentioned above leads to information superiority essential to maintain an advantage against the adversary.

The meshed WiFi technology described below can be integrated with unmanned aerial vehicles (UAVs), for example, to create or extend a "WiFi Cloud." UAVs could be used to create an over the horizon (OTH) communications relay or surveillance capability in an operations area that is constrained by terrain and widely dispersed forces. WiMAX bridge technology is also discussed, which can link two geographically separated areas easily up to 50 kilometers from each other, using point-to-point, point-to-multipoint and multipoint-to-multipoint wireless configurations.

Leveraging the HFN wireless infrastructure, the Royal Thai Navy (RTN) was able to train and field test the Android-based Lighthouse application with personnel from the

NPS Common Operational Research Environment (CORE) Lab. The Lighthouse application is a mobile data collection, social network analysis and geospatial display tool that supports counter-improvised explosive device (C-IED) activities and village stabilization operations (VSO).

The discussion below represents the wireless concepts and technologies that were used during the ten day experiment with RTARF counterparts.

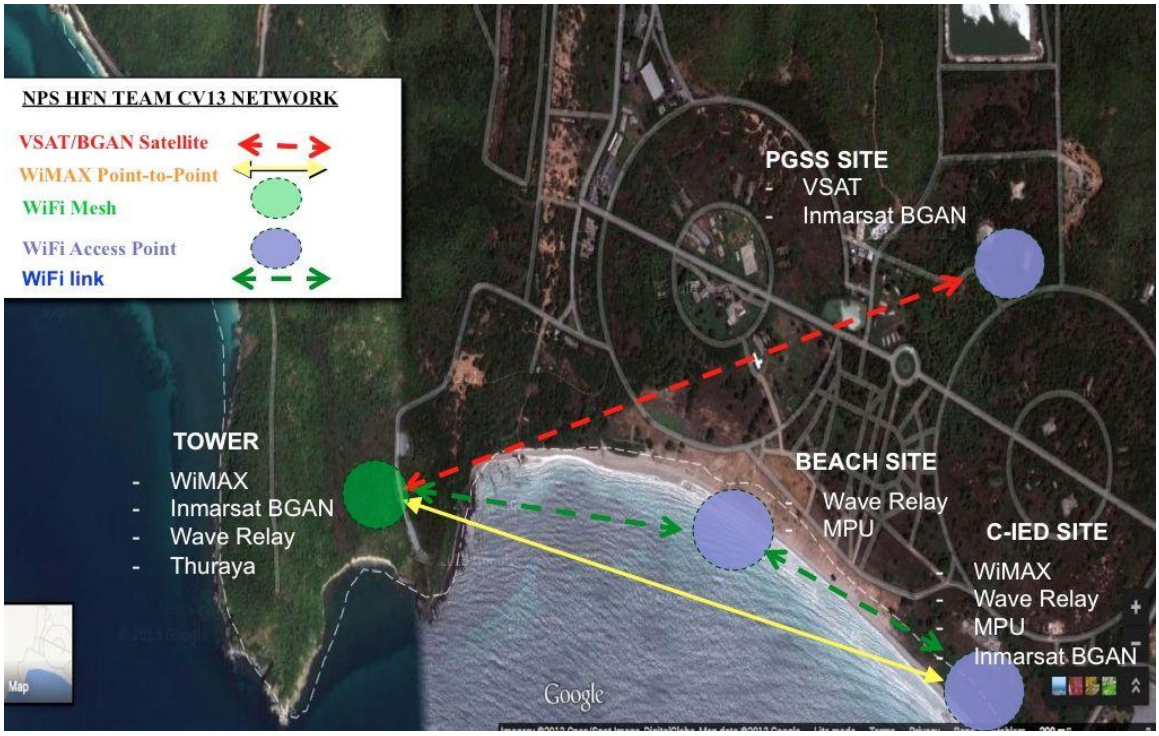

Figure 9. Crimson Viper 2013 Wireless Network Footprint–Hat Yao, Thailand

A. WIRELESS AD HOC NETWORK CATEGORIES

A wireless ad hoc network is typically deployed without a requirement for preexisting infrastructure (e.g., wired networks, routers, or access points) and is generally decentralized. Data routing is done individually by each node, for the other nodes that are established, resulting in a dynamic establishment of nodes that forward data according to the network's connectivity. Typically, wireless ad hoc networks serve a temporary purpose in support of specific missions that do not require a permanent communications

infrastructure. Although they can also be deployed for longer periods than what the original mission called for (Kontogiannis, 2012, p. 9).

Several descriptions are used to capture the concept of Ad hoc networking. These include: self-organizing, self-healing, self-balancing and self-aware. The main premise behind a self-organizing network is the ability to form a larger network as the ad hoc network itself comes into contact with another wireless network, or "cloud" (Valentine, 2005, p. 70). This is extremely useful for military units involved in operations that have a constantly changing scheme of maneuver, since the connectivity through the network is retained even though one or more participating nodes may fail, move out of range, or have their propagation paths temporarily blocked due to terrain or physical barriers.

1. Wireless Mesh Networks

A wireless mesh network (WMN) is defined as a communications network consisting of nodes that are structured in a mesh topology. In a mesh topology, the nodes of the network have point-to-point connection with the remaining nodes of the network. Each node transmits data to other nodes. This ensures that the information flows seamlessly within the network as the data is able to reach its final destination through alternate communications paths (Kontogiannis, 2012, p. 7). With a wireless mesh network, each network cloud is aware of its surroundings and can collectively decide the optimum path to best send data across the network to maximize throughput (Figure 9). If a specific path is either lost or weakened, an alternate path is automatically selected – a process known as "self-forming." As more nodes are introduced into the cloud, the network strength increases (Valentine, 2005, p. 71). As nodes are added into the network, they will self-organize and self-heal. This process allows for the continuous use of the network so that information can be shared without any delays or interruptions.

WMNs can enable IEEE 802.11 and 802.16 standards. Mesh networks, because of their ability to self-heal and organize, provide scalability, allowing coverage over wider geographic areas. Because of the multiple nodes involved, a WMN is highly reliable and, certainly redundant. They also provide a cost-effective means of extending the enterprise as connectivity is spread among multiple mobile users that have specific requirements to access applications (Kontogiannis, 2012, p. 7).

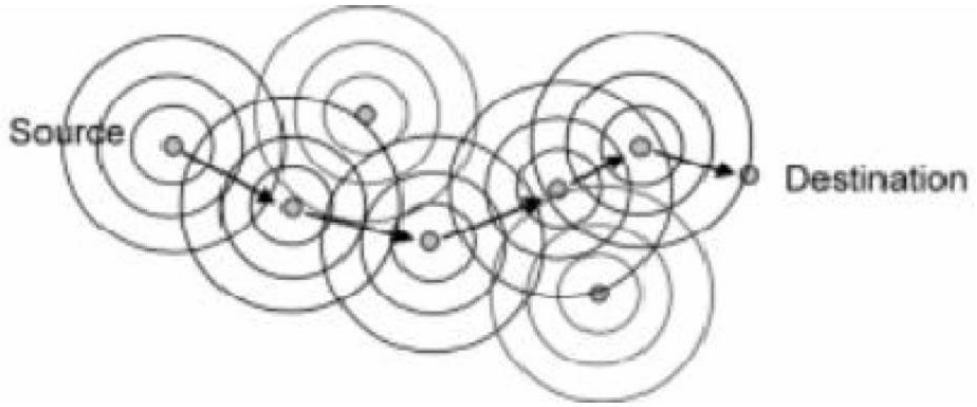

Figure 10. Wireless Mesh Network(from Valentine, 2005)

2. Mobile Ad Hoc Networks

A MANET, according to the *Advanced Network Technologies Division of National Institute of Standards and Technology (NIST),* is defined as "an autonomous collection of mobile users that communicate over relatively bandwidth-limited wireless links" (NIST, 2012). Due to the mobility of a MANET's nodes, particularly during military maneuvers, the network topology may assume various configurations that were not initially planned (Kontogiannis, 2012, p. 8). Because MANETS are mobile, they use wireless connections to form a self-configuring network that communicate using multi-hops within nodes. The wireless connections can be standard WiFi, cellular or satellite connectivity. The constant mobility of the nodes distinguishes the MANET from a WMN in which the nodes are less mobile and sometimes permanent.

MANETs are also decentralized and do not require existing infrastructure or regulated connectivity (2012, Menjivar, p. 40). However, there are various issues that adversely impact the communications link such as topology, interference, propagation and attenuation (Kontogiannis, 2012, p. 8).

In military operations (Figure 10), MANETs need to have the ability to overcome constraints in connectivity, bandwidth, communications security, power and scale. Other issues such as reliability, jamming, latency and network failure recovery must be considered in planning the MANETs design and performance (Kontogiannis, 2012, p. 8). Military networks are also designed to operate in ways that assures low probability of

intercept and detection. As such, the nodes need to be configured so as to discharge the least amount of power and moderated transmission frequency so as to evade the adversary's sensors. A departure from these specifications may result into the degradation of the network's performance and credibility (Kontogiannis, 2012, p. 9).

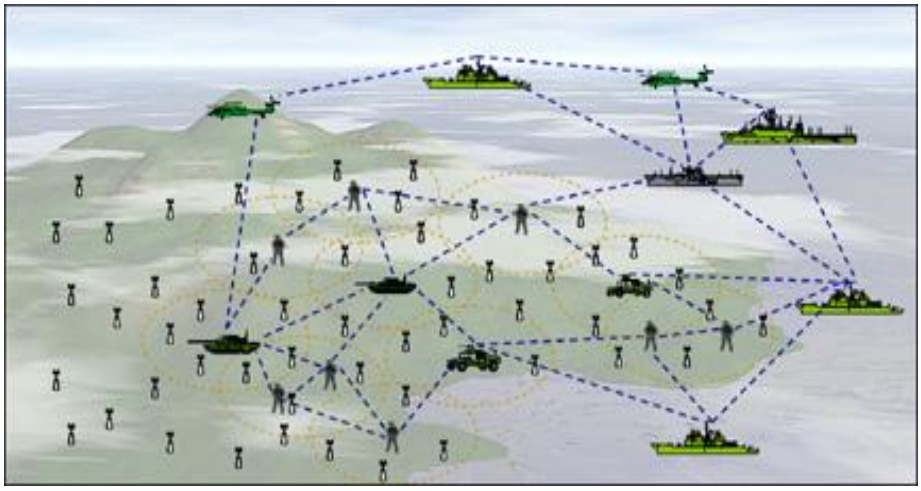

Figure 11. Mobile Ad Hoc Network (from Kontogiannis, 2012)

3. Wireless Ad Hoc Sensor Networks

A wireless ad hoc sensor network (WSN) is one of the most robust types of networks for wireless communications particularly for military use. WSN's consists of a number of sensor nodes spread across a defined geographical area (2009, Misra). The NIST definition states that "each sensor node has wireless-communication capability and some level of intelligence for signal processing and dissemination of data" (NIST, 2012).

WSNs are distinct from WMNs or MANETs since their primary application is not limited to communications, but they have the added advantage of data gathering through integrated sensors that can be shared throughout the network (Kontogiannis, 2012, p. 14).

The following list extracted from the NIST website contains examples of how wireless sensor networks are applied:

- Military sensor networks for surveillance and detection of enemy movements or other important phenomena like explosions

- Sensor networks for detection of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials or attacks
- Wireless-sensor surveillance networks for providing security in public places or other facilities monitored by authorities or security companies
- Detection of explosives during an IED attack

In a study by V. Krishnamurthy, on *Emission Management for Low Probability Intercept Sensors in Network Centric Warfare*, he writes

> The information for generating battlespace awareness in NCW is provided by numerous sources, for example, stand-alone intelligence, surveillance, and reconnaissance platforms, sensors employed on weapons platforms, or human assets on the ground. In the fundamental shift to network-centric operations, sensor networks emerge as a key enabler of increased combat power. The operational value or benefit of sensor networks is derived from their enhanced ability to generate more complete, accurate, and timely information than can be generated by platforms operating in stand-alone mode. (Krishnamurthy, 2003, p. 2)

Certainly, the unique capabilities that are derived from wireless network sensors are indisputable. They have a wide-range of military applications that enhances situational awareness that results in superior decision-making. In a dynamic and constantly evolving operational environment, the ability to sense the situation around you and share that awareness, creates a more effective force that can act in unison and with shared understanding of the terrain, weather, demographic conditions and enemy intent.

B. HFN NETWORK COMPONENTS

1. 802.16—Worldwide Interoperability for Microwave Access

WiMAX is a long-range wireless communications technology that is based on the IEEE 802.16 standard. It is generally viewed as the "last-mile" solution that expands broadband connectivity to rural areas and cities through a robust wireless link (Hwee, 2007, p. 55). WiMAX antennas are known for their compactness, flexibility and rapid installation. Additionally, these antennas can be mounted on poles and are generally weatherproof. WiMAX are usually deployed to provide coverage to areas that can extend up to 50km. A mobile user does not need specialized software to gain connectivity as the technology itself assures a persistent, high-speed wireless connection.

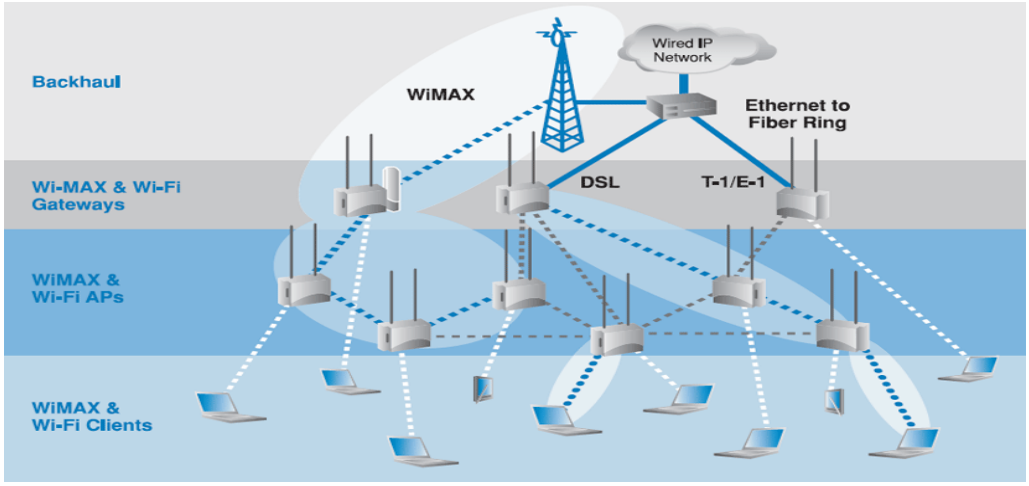

Figure 12. WiMAX Network Architecture

a. WiMAX Wireless Configurations

Given the terrain and remoteness of rural areas in southern Thailand, the ideal tactical network should be based on wireless LAN and meshed technologies that do not require a physical data transportation infrastructure (Figure 11). This solution is a more cost-effective approach compared to conventional communication technology, as it does not require running cables for communications reach back. There are three wireless configurations that can be employed: Point-to-point, point-to-multipoint, or multipoint-to-multipoint. It is important to understand the differences between these configurations to effectively employ the best tactical network that can cover a wider area of operations without the restrictions associated with an area's physical terrain.

(1) Point-to-point Configuration

A point-to-point wireless configuration is simply two stations communicating with each other (Figure 12). It is not efficient for multicasting or sharing of information with multiple stations. True "networking" does not take place.

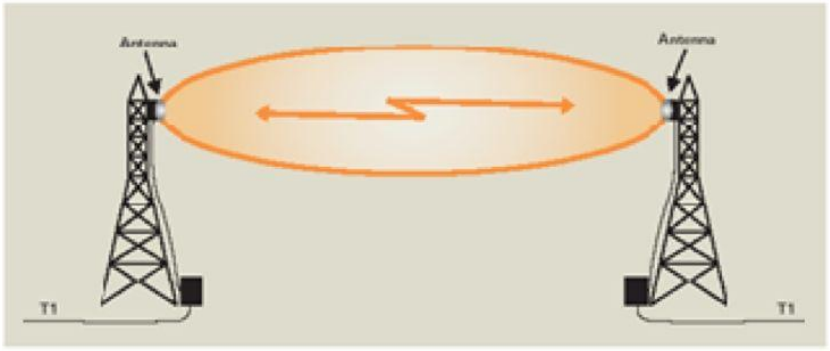

Figure 13. Point to Point Network

(2) Point-to-multipoint Configuration

Point-to-multipoint wireless networks are generally constrained because of the lack of interaction among the clients within the network (Figure 13). Data transmission only occurs between sender and receiver, however, not among the nodes in the network (Valentine, 2005, p. 69).

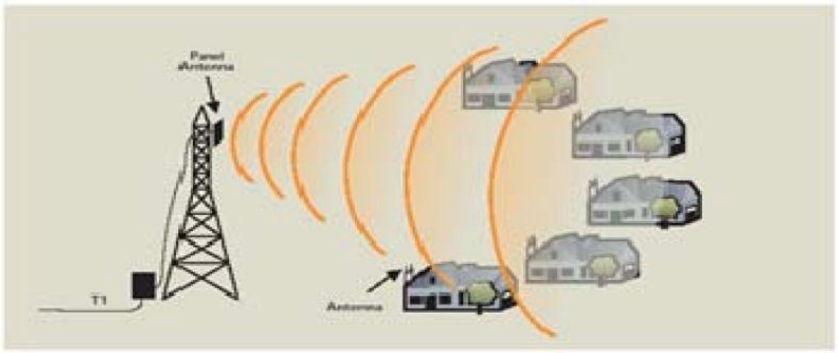

Figure 14. Point to Multi-Point Network

(3) Multipoint-to-multipoint Configuration

The multipoint-to-multipoint topology is the preferred wireless configuration for military applications. In this configuration, every node becomes a router within the network, which enables a much wider coverage and allows for the formation of ad hoc networks (Figure 14).

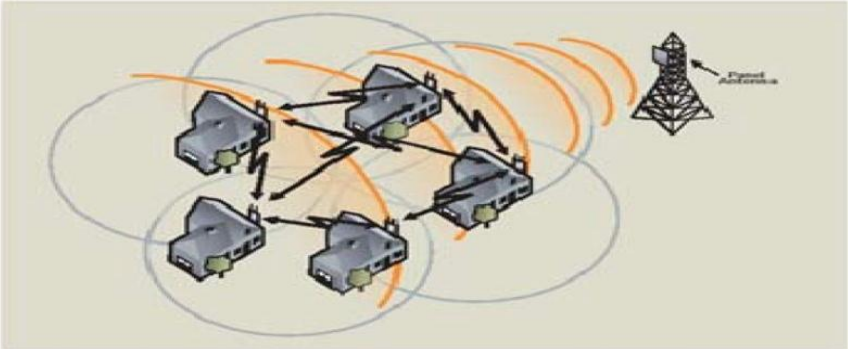

Figure 15. Multi-Point to Multi-Point Network

The 802.16 standard was designed to provide permanent broadband wireless access in a local area network (LAN) or metropolitan area network (MAN) environment (Intel, 2005). It operates in the 10 and 66 GHz frequency range and has the same performance similar to Digital Subscriber Line (DSL) or T1 systems. Data transfer rates for line-of-site (LOS) transmission using the 10-66 GHz frequency range, approaches 120 Mbps while non-LOS transmissions in the 2-11 GHz frequencies are 70 Mbps (Leeper, 2005). Overall, 802.16 systems provide a reliable alternative to wired systems as they are generally cheaper to maintain (no use of fiber optic or CAT-5 cabling), ease of setup (plug and play capability) and broader coverage of specific areas because of the long range and scalability..

During the Crimson Viper 2013 experiments in Hat Yao, Thailand, two WiMAX links were set up approximately two miles apart (Figure 15). The link was established in less than thirty minutes and a WiFi mesh was immediately established to support various operations. Internet reach back was provided through Broadband Global Area Network (BGAN) portable satellite and very small aperture terminal (VSAT) units at two separate locations which will be discussed in the next section.

In a similar NPS field experiment in Thailand known as Coalition Operating Area Surveillance & Targeting System (COASTS) that was conducted in Thailand in 2005, two 802.16 links, six kilometers apart were set-up and achieve full operational capability in under two hours (Valentine, 2005, p. 73). According to the after action report from the 2005 COASTS experiment, large amounts of video, sensor data and network information

was delivered over the network with a high degree of speed and accuracy, due to the large bandwidth available. The combined cost of the equipment (provided by Redline Communications) required to operate these two links was approximately $30,000 USD. This cost compares favorably with the costs of laying fiber-optic cable, which is approximately $20,000 USD per mile in Thailand (Valentine, 2005, p. 74).

Figure 16. WiMAX Antenna Deployed in Hat Yao, Thailand

2. 802.11 Wave Relay MANET

Wave Relay is a "Mobile Ad Hoc Networking system (MANET) designed to maintain connectivity among devices that are on the move" (2014, Persistent Systems). It is a peer-to-peer mesh networking solution, using a proprietary algorithm, designed for forces that are deployed in difficult and austere environments, but have a requirement for robust communications connectivity that is also secure and dynamic. According to its manufacturer, Persistent Systems, it is a scalable system that has a throughput of 41 Mbps UDP and 31.1 Mbps TCP. It uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) which avoids collisions by only transmitting after the channel is detected to be in idle mode (Chatzigiannis, Gibson & Singh, 2012).

For the Crimson Viper 2013 field experimentation in Thailand, there were two models used: the Quad Radio Router and the Man Portable Unit Gen4 (MPU4) with the

tethered Android kit. Two (2) Wave Relay Quad Radio Routers were set up; one unit at the network operations center (NOC) and the other was located at the beach within close proximity to the U.S. and Royal Thai Navy (RTN) explosive ordnance disposal (EOD) team's base of operations. Two (2) MPU4's were deployed separately with two EOD units in support of the IEDNA (Improvised Explosive Device Network Analysis) experiment using the NPS Lighthouse technology.

a. Quad Radio Router

The Wave Relay Quad Radio Routers (Figures 16–18) are MANET wireless devices packaged in compact ruggedized cases, which may be used to implement a large geographic coverage network. They have a range of more than two miles using an omnidirectional antenna, and a 27Mbps maximum throughput on TCP and 37Mbps on UDP, using a 20MHz channel (2014, Persistent Systems). Each unit contains four separate wireless radios with the ability to perform package routing functions. Each Quad Radio operated may be procured in one of several frequencies, to include but not limited, to 700 MHz, 900 MHz, 2.3-2.4 (S-Band) GHz, and 5.8 GHz (C-Band) (2014, Persistent Systems). The router has a proprietary algorithm that selects the strongest signal path to communicate with neighboring nodes.

Figure 17. Wave Relay Quad Radio Router

Figure 18. Quad Radio Router #1 at the JOC, Hat Yao, Thailand

Figure 19. Quad Radio Router #2 on the beach in Hat Yao, Thailand.

b. Man Portable Unit Gen4 (MPU4)

The MPU4 is a portable and lightweight 802.11 radio (Figure 18), which operates between 700 MHz and 5 GHz frequency range. It provides MANET capability directly to units that operate in austere environments and difficult terrain. The MPU4 utilizes a standard military battery that according to its manufacturer "*provides 14 hours of run-time and enables customers to reuse batteries and chargers that are already in their supply system*" (Persistent Systems, 2014). It also supports peer-to-peer network topology, real-time position location through a connected GPS and serial data transmission to participating network nodes. With the high data bandwidth that it uses, it is able to provide up to 37 Mbps of throughput supporting voice (up to sixteen press-to-talk (PTT) channels), video, and data communications (Persistent Systems, 2014). The MPU4's effective range with the use of an omnidirectional antenna is approximately two nautical miles with a peak transmission power of two watts.

Figure 20. Wave Relay Man Portable Unit Gen4 (MPU4)

A wireless mesh that integrates both WiMax and Wave Relay systems (shown in Figure 18) provides the best option in both long haul and short-range connectivity. Table 5 shows a comparison of the technical specifications between these two systems.

	WiMAX	Wave Relay
Maximum Range (km)	80	24.3 (40MHz channel), 52.5 (20Mhz channel)
Maximum throughput	90 Mbps	27Mbps (TCP), 37Mbps (UDP)
Encryption	AES-128, AES-256	AES-CTR-256 with SHA-512 MAC
Channel size	40Mhz	40Mhz
Max Tx power	25dBm	28dBm (civilian version), 33dBm (military version)
Antenna Gain	16dBi (120° sector), 9dBi (omni)	14dBi (120° sector), 5dBi (omni)
Frequency	5.8Ghz	2.3-2.5Ghz and 5Ghz

Table 4. WiMax versus Wave Relay (from Morris, 2011)

3. Broadband Global Area Network

The Broadband Global Area Network (BGAN) was created in 2006 and was designed to be transported by a single person and able to connect to a satellite within minutes. The network is provided by the British satellite telecommunications company, Inmarsat and uses three geostationary satellites to provide global coverage.

BGAN allows any mobile device with wireless capabilities to connect to the internet because of its dynamic host control protocol (DHCP) capability that automatically provides devices with a unique internet protocol (IP) address, allowing them to use the BGAN's WiFi cloud after entering the requisite wireless encryption protocol (WEP) key. This key feature allows several mobile users to utilize the BGAN to accomplish operational tasks. Figure 20 shows the Inmarsat I-4 satellite coverage area along with the corresponding look angles. Theoretically, the Inmarsat footprint covers most of the world with the exception of remote polar regions.

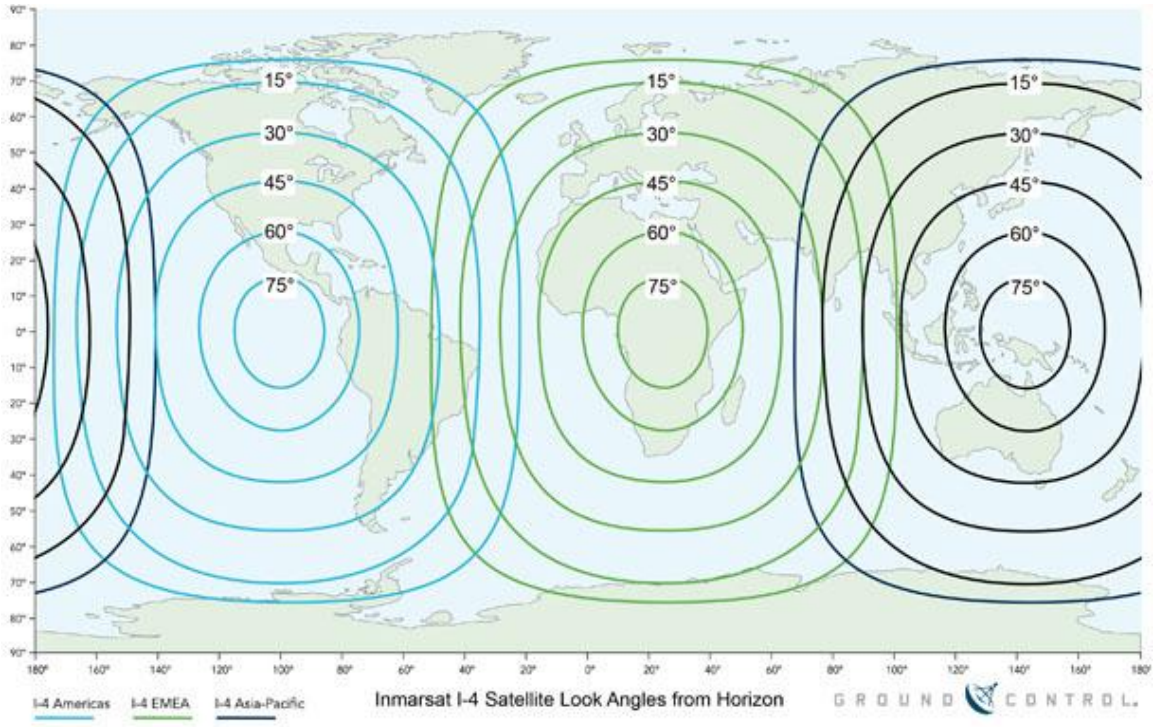

Figure 21. Inmarsat BGAN Coverage Map with Look Angles (from Inmarsat, 2014)

BGAN satellite terminals are ideal for RTARF troops traveling in remote southern areas because of its light weight and ease of use. Additionally, they are ruggedized and some models such as the Hughes 9201 also come with the ability to broadcast a WiFi signal within a 100-meter circumference area, creating a WiFi cloud for mobile devices. This capability provides small RTARF teams the ability to operate in remote rural areas while maintaining Internet connectivity. Critical command and control functions are assured through various communication methods such as email, voice over internet protocol (VoIP) applications such as Viber or Skype, simple mail service (SMS) text messaging and virtual private network (VPN) services.

The BGANs used during the Crimson Viper 2013 experiment were the Hughes 9201 (Figure 21) and 9450 on-the-move satellite terminal (Figure 22). The Hughes 9201 is a lightweight, portable device which can be carried in a shoulder bag or briefcase.

Figure 22. Hughes 9201 BGAN satellite terminal

The Hughes 9450 satellite terminal (Figure 22), also known as "BGAN In-motion" is a mobile unit that can be magnetically mounted on a vehicle's roof. There is a built-in tracking antenna that automatically maintains satellite connectivity while the vehicle is in motion. The Hughes 9450 BGAN terminal is ideal for use in RTARF command vehicles that have the need for constant movement but require internet reach back capability and command and control functions.

Figure 23. Hughes 9450 Mobile Satellite Terminal

According to the company Inmarsat, the BGAN satellite terminals have the capability of transmitting data at an uplink and downlink speed of up to 492 kbps (Inmarsat, 2011). However, this speed can only be reached with the X-stream capability. On connections with the satellites, the user must specify the connection speed of 32, 64, 128, 256 kbps, or X-stream. Once connected and the link has been established, multiple users can use the device via the built in WiFi access point.

While testing the Hughes BGAN in Hat Yao, Thailand during Crimson Viper 2013, the highest uplink speed obtained was 79 kbps and the fastest download link was 54 kbps. The signal strength to the satellite was 100% and the speed chosen was 256 kbps. The weather was clear with no physical interference.

Figure 24. Hughes 9201 BGAN Terminal Connected to a WiMAX Antenna (from Crimson Viper 2013, Hat Yao, Thailand)

The BGAN does have some drawbacks and limitations. First, it is required to run on Subscriber Identity Module (SIM) cards. The SIM cards are only good for a designated amount of download bandwidth and can be used up quickly creating a need to carry multiple SIM cards each time the BGAN is used. Second, the cost to use the device is much greater than the VSAT because it is based on data usage versus flat monthly fees, typically around $4 to $7/Mbyte (Inmarsat, 2014). BGANs are also reliant on line of sight (LOS) connectivity to the satellite. This drawback may be an issue for RTARF forces that are deployed in major population centers that have tall buildings and infrastructures or even remote mountainous areas with large trees and multiple obstructions. Maintaining a reliable communications link may be challenging due to these conditions (Morris, 2011, p. 46).

4. Thuraya IP Data Terminals

The Thuraya IP data terminal (Figures 24-25) is an advanced dual-mode GSM cellular/satellite device, designed and built by Hughes for the Thuraya satellite system gateway. Thuraya, is a telecommunications company based in the United Arab Emirates, which according to its website, has a satellite network that covers more than 120 countries including the world's remotest locations, ensures congestion-free satellite communications and connectivity at all times through its "always-on" network access (2014, Thuraya).

The product that was tested during the Crimson Viper field experimentation in Thailand was the Thuraya IP Plus, an ultra-light weight (weighing 1.4 kilograms) and compact satellite modem that according to the company, "is the world's smallest, highly portable and most durable satellite terminal" (Thuraya, 2014). Although not specifically measured during the exercise, the datasheet extracted from the Thuraya website shows that the terminal is capable of providing data rates of 444 kbps on standard IP and 384 kbps using streaming IP. These speeds provide enough throughput to support various internet-based applications such as VoIP, email services, video conferencing and broadcast and web browsing. The Thuraya IP terminal has a rugged design and is compliant with the IP 55 protection standard. This makes it ideal for use in rough weather and austere environments – conditions that the RTARF forces continuously encounter in the remote areas of southern Thailand. The dual mode

functionality also allows RTARF users to switch to the GSM mode to take advantage of the area's existing GSM cellular infrastructure.

Figure 25. Thuraya IP Data Terminal

Figure 26. Thuraya IP Data Terminals at the CV13 NOC, Hat Yao, Thailand

5. Very Small Aperture Terminals

VSATs were also used during the Crimson Viper field experiment and were specifically located at the persistent ground surveillance system (PGSS) area of operations. The NPS Hastily Formed Networks Center has successfully deployed VSATs with its disaster response teams during the Asian tsunami in 2004, Hurricane Katrina in 2005, Haiti's earthquake in 2010 and most recently, during the aftermath of Typhoon Haiyan in the Philippines in 2013. Because of their mobility, high throughput and

applicability in remote and austere environments, supporting voice, data and video streaming functions, VSATs (shown in Figure 26), can be a robust reach back option for the RTARF in southern Thailand.

Figure 27. Tachyon Network VSAT Terminal

Although not as portable as the BGAN or Thuraya satellite terminals, VSATs offer enough mobility since the size of their dish antennas do not normally exceed three meters. The vast majority of VSAT dish antennas range between 75 centimeters to 1.2 meters. What makes VSAT terminals compelling is the throughput, which range from 4 kbps to 16Mbps. The satellites used by VSAT terminals are in geosynchronous orbit and operate in the X, C, Ka, and Ku bands and can connect to an array of satellites.

Additionally, the VSAT network can be deployed in one of three configurations:

(1) Star Topology

This is a configuration where a network operations center (NOC) is utilized as a hub or main uplink site, to transmit data between deployed VSAT terminals through the satellite. If a remote VSAT terminal intends to transmit data to another terminal in the network, it would have to send the data packets to central NOC. This is known as a "double hop" link using the satellite (Figure 27).

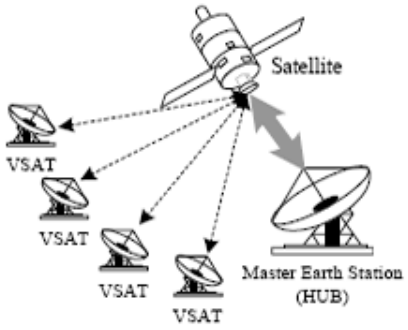

Figure 28. VSAT Star Topology

(2) Mesh Topology

With this configuration, each VSAT in the network can transmit data packets directly to any VSAT terminal within the network. Unlike the star topology, a central uplink site like a NOC is not required as all the terminals share network control duties (Figure 28).

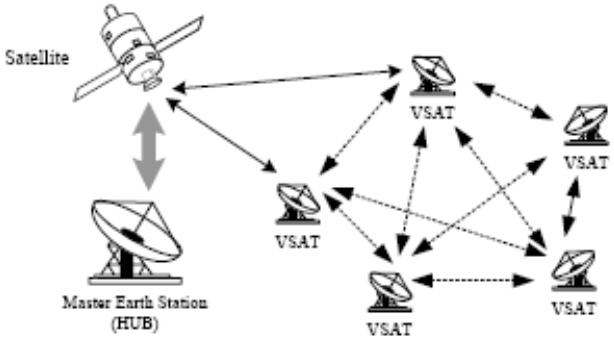

Figure 29. VSAT Mesh Topology

New commercial VSAT systems such as Inmarsat's GlobalXpress (figure 29) are entering the marketplace and leverage Ka band technology. Ka band operates in the 26.5–40 GHz frequency range and offers higher bandwidth communications.

Figure 30. Inmarsat GlobalXpress (from Inmarsat, 2014)

VSAT commercial satellite communication systems present a convincing value proposition, particularly for developing countries like Thailand who may find launching and maintaining their own satellite constellation, cost prohibitive and untenable.

6. Reusing Existing Natural Energy, Wind and Solar (RENEWS)

Operating networking equipment and mobile communications effectively requires a reliable power source. Remote environments that are typical in the Asia-Pacific region are usually outside the reach of a country's electrical power grid. Most military operations are away from urban centers and typically rely on fossil fuel generators to power their equipment. In the insurgent infested areas of southern Thailand, supply routes are usually vulnerable to attacks. So securing supply lines with personnel and resources that are already stretched thin becomes a priority for RTARF planners so they can deliver fuel and critical logistics to remote units. Units stationed in remote rural outposts face significant challenges in powering their electronic devices. Without fuel to power military equipment, the idea of network centric warfare using HFN technology is rendered ineffective for counterinsurgency operations.

During the Crimson Viper 2013 exercise, the U.S. Army contingent demonstrated the Reusing Existing Natural Energy, Wind and Solar (RENEWS) system (Figures 30–32). RENEWS is a self-sustaining system that completely relies on renewable energy sources such as solar and wind. The system was designed to provide reliable power to small teams operating in remote areas where fuel re-supply becomes challenging or in some cases,

outright dangerous. The power requirements of these units are minimal since they normally operate communications equipment that are smaller in size and require less power.

According to the *U.S. Army's Command, Power & Integration Directorate*, "RENEWS is designed to produce up to 300 watts, enough to power portable communications equipment continuously as long as there is power coming daily from the solar panels or wind turbine. The storage component provides power at peak demand for about five hours when energy is not being generated by the renewable components. The RENEWS components weigh about 100 pounds, and it is stored in two cases weighing about 70 pounds each" (U.S. Army, CERDEC, 2014).

The NPS HFN research team in partnership with U.S. Army personnel, field-tested the RENEWS components in Hat Yao, Thailand and found the flexible solar panels and wind turbine to be effective in powering the HFN wireless mesh.

The team set up the RENEWS components in each of the following locations:

(1) Crimson Viper JOC (Figure 30)

(2) C-IED site (figures 30 and 32)

The two sites were approximately two miles apart and had the standard HFN fly-away kit composed of one (1) 802. 16 WiMAX radio/antenna, one (1) Wave Relay 802.11 quad radio wireless access point, one (1) Wave Relay MPU4, one (1) laptop and six (6) BB-2590 rechargeable lithium ion military batteries. Each site was powered completely by three 90W flexible solar panels and the wind turbine. Each site was able to operate continuously for eight hours without ever tapping into the electrical grid.

This proves that integrating RENEWS with HFN equipment helps alleviate the dependence on using fossil-fuel generators in remote areas. By reducing the amount of consumable resources being used, and relying more on natural alternatives such as wind and solar energy eases the transportation and security burden of operating in southern Thailand.

Figure 31. RENEWS at Hat Yao JOC site

Figure 32. RENEWS with WiMAX and Wave Relay AP at C-IED Site

Figure 33. RENEWS Wind Turbine and Solar Panels at Hat Yao Op Area

7. Unmanned Aerial Vehicles as Aerial Nodes

Although UAVs are outside the scope of the current HFN technology implementation, it is important to consider the concept as it extends the capabilities of existing wireless systems, increasing their range and coverage area. HFNs using UAVs as aerial nodes (Figure 33) provide the flexibility to extend the HFN wireless mesh beyond the horizon and throughout the uneven terrain typical to the RTARF operating areas. Over the horizon (OTH) communications are an integral part of network centric operations: it overcomes terrain restriction and optimizes the coverage of a network for multiple ground units spread over a large area.

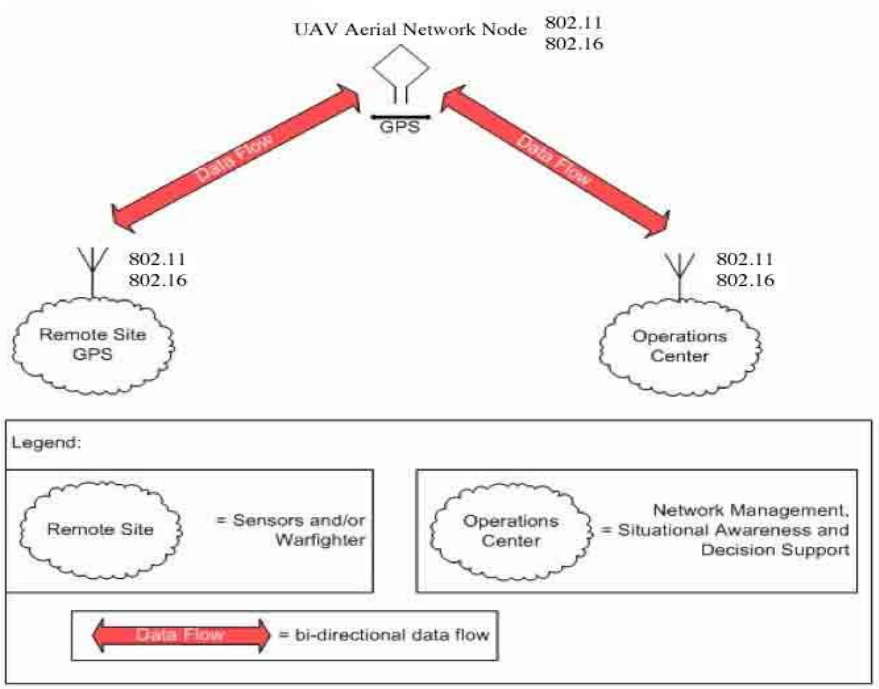

Figure 34. UAV Aerial Network Node (from Hubbard, 2002)

The modern warfighter is equipped with numerous tools that enhance his/her situational awareness, such as communications gear, targeting tools, computer displays and various technologies that make him/her information-enabled. Utilizing these different elements requires a greater network signal footprint, in order to extend the command and control that the unit commander can exercise. Furthermore, a UAV acting as a wireless aerial node with long loiter times can provide "local persistence." Local persistence allows continuous availability of intelligence data. This allows the on-site commander to access information obtained directly through organic units and distribute this information through the HFN wireless mesh.

a. UAVNET

Traditionally, UAVs have been used by the military for surveillance and reconnaissance operations, with military classifications of UAVs falling under three tiers. Tier I UAVs are ship or battlefield-launched and designed for quick response missions. Tier II UAVs such as *Global Hawk* and *Predator*, are designed for endurance operations at medium altitude. Tier III UAVs, such as *Dark Star*, are high-altitude cruising vehicles

designed for low observability and greater endurance. All three of these types are over-kill for the purposes of HFN; they are expensive, require considerable infrastructure to support for both operations and maintenance, and are unable to exercise the kind of time-on-station within very constrained operating space necessary for the proposed mission.

With the advent of robust wireless networking technologies, particularly those based on the 802.11 and 802.16 standards, and taking advantage of commercially available smaller and more portable vehicles, UAVs can be equipped with wireless transceivers and thus enabled to communicate with ground nodes as well as other UAVs.

The following scenarios are based on a framework called UAVNet that originated from the Institute of Computer Science and Applied Mathematics, University of Bern in Switzerland. According to the experiment, "UAVNet is a highly adaptive and mobile WMN using small UAVs. It includes a concept and a prototype implementation of an autonomously and temporarily deployable WMN, using UAVs with attached wireless mesh nodes. The deployed communication network enables the connectivity between different end systems like notebooks, smartphones and tablets and even other wireless or wired networks" (Morgenthaler et al, 2013).

Two of the three scenarios below have been borrowed from the University of Bern research, with the third being our own theoretical scenario.

(1) Airborne Relay Scenario with a Single UAV

In this first scenario, only a single UAV is needed to establish a communications link, connecting two users at separate locations. The UAV would operate autonomously and fly between the two locations, while using the wireless mesh to forward packets of data between the two end points. The UAV starts in an area close to the first location and broadcasts ping messages on a regular basis. As the first location receives the packets, it sends a GPS signal to the UAV, so it can determine its exact location. Once the UAV determines the GPS coordinates, it begins to fly toward the first location in a spiral track while it simultaneously searches for the second location by broadcasting similar ping messages. Once the second location receives the UAV ping, it also sends its own GPS signal for the UAV to track. So in theory, the UAV simply flies autonomously between

the two end points as long as a persistent communications link between all three assets are established. The UAVs flight control systems (FCS), allows the UAV to calculate relative distances between the two locations and determine the center position between the two, to maximize the effective range between both end points and efficiently act as an aerial relay for both locations.

(2) Airborne Relay Scenario with Multiple UAVs

In situations that require wider network coverage, a single UAV may not be sufficient to bridge the distance between two or more locations; so multiple UAVs may be required to create a communications relay. Using the wireless mesh nodes, several UAVs can form a chain to transmit data packets between two locations. The scenario, theoretically works as follows:

(1) A single UAV starts the chain and serves as the scout to spot the location of the first user, using a similar search algorithm described in the first relay scenario. Once the UAV approaches the location, it broadcasts a GPS signal so all the other UAVs in the chain so they can proceed to the location of the first user.

(2) Once the first phased is accomplish, the first UAV will then approach the second user's location based on the GPS signal broadcast from the second user. Alternately, the UAV will also relay the GPS coordinates of the second user to the UAV chain. The UAV will then take a position that is centered between the two locations.

(3) Once the first UAV arrives at center point, it flies back to the first location and determines the signal strength value and stay in place as its final position.

(4) The second UAV approaches the location of the first UAV and moves back toward the direction of the second location until it receives the signal strength relative to the first UAV;

(5) This process is repeated with the rest of the UAV chain until each UAV is properly positioned to ensure optimal connectivity. UAVs can hover at different altitudes to avoid collision.

(3) Airborne Mesh Network Scenario with Multiple UAVs

Rather than building a straight-line relay that essentially connects two endpoints, we propose a more robust approach to a hastily formed mesh network - to take on an additional dimension. Using a large collection, or swarm, of multi-rotor UAVs (vice the traditional fixed-wing variety), a HFN may be formed over a physical space that covers wide areas of operations, blanketing the battlefield under an umbrella of network connectivity. Rather than being programmed to seek out end users and take up a position relative to them, the network nodes (and specifically the UAVs used to transport them) would use controlling software that enforces positioning relative to surrounding nodes. Minimum acceptable operational distances could be established as a means of ensuring redundancy (limiting separation of nodes increases overlap between nodes), and therefore maximize connectivity. Individual UAVs would not require a unique pilot for each one, and instead could rely on a centralized controlling unit. Using a simple graphical user interface (GUI), entire groups of UAVs could be controlled as a single unit, with formations being either user-defined or pre-programmed and switchable in real time. With UAVs maintaining constant positional data with respect to one another, as well as onboard GPS data, the entire network could be mobilized to cover either an area relative to the controlling unit (or other designated unit of interest), or to cover a specific geographic region. End users would be able to join their devices to the network regardless of which node they were in the vicinity of, and devices could intelligently select which node to connect to for most efficient delivery of data.

UAVNet has some significant advantages compared to ground-based networks, as it is not restricted by environmental constraints due to terrain. Additionally, the inclusion of nodes that are not only self-healing with respect to network protocol management, but also self-guiding and self-propelled with respect to their physical orientation in the real world makes them ideal for near-autonomous network communication infrastructure. This provides the ability to extend the network over the horizon to cover a larger geographic area not typically achieved by ground based systems, while simultaneously limiting the number of personnel required to establish, operate, and maintain a network.

8. Lighthouse Technology

Lighthouse is a suite of applications and a methodology developed by the Naval Postgraduate School's Common Operational Research Environment (CORE) Lab. The CORE Lab itself is essentially an intelligence fusion center for NPS defense analysis students who help solve real-world problems they encountered in the field. The vast majority of these students come from the special operations community.

The concept behind Lighthouse technology is to leverage open source, social network analysis, temporal records, geospatial data and relational analysis to create a common operational picture (COP) so military commanders can make informed decisions (Figure 34). Lighthouse is an effective tool in counter-improvised explosive device (C-IED) operations as proven by its success in Iraq and Afghanistan. By structuring data already being collected and applying social network analysis, explosive ordnance disposal (EOD) units can rapidly and efficiently develop a broader understanding of the IED networks that they are trying to pursue. Better information leads to a better strategy of targeting and eliminating IED networks that wreak havoc on troops and the community at large.

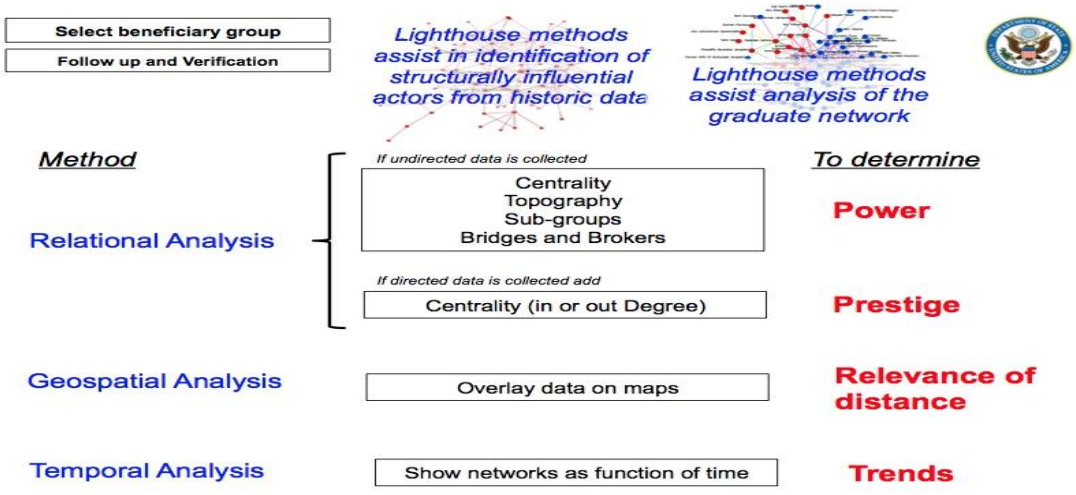

Figure 35. Lighthouse Methodology (from NPS CORE Lab, 2014)

a. Lighthouse Analytical Components

(1) Social Network Analysis (SNA)

In a report by Katherine Zimmerman titled *The Al Qaeda Network: A New Framework for Defining the Enemy*, she describes the "leaderless worldwide jihad," which is a shift in how terrorists, insurgents and various non-state actors organize worldwide. This new framework undercuts the idea of the importance of hierarchy and top-down directives. According to Zimmerman, "the concept of leaderless worldwide jihad minimizes the significance of the core leadership group and emphasizes decentralization and bottom-up operational initiative" (2012). The lack of centrality in this new terrorist framework makes it more difficult to defeat non-state armed groups, as simply targeting central individuals in the network, do not necessarily weaken their organization (Zimmerman, 2012). According to the same research, this new model makes insurgent organizations more resilient and less vulnerable, which presents a new conundrum for military planners.

However, to solve this new dilemma, Sean Everton, a professor in the Defense Analysis Department at NPS, proposes the use of social network analysis (SNA) to understand the human terrain and the ties between insurgent actors to craft strategies to track, destabilize, and disrupt terrorist and insurgent networks. Everton's book, *Disrupting Dark Networks*, is the first book in which counterinsurgency theory and social network analyses are coupled. Social network analysis, according to a research titled *Targeting: Social Network Analysis in Counter-IED Operations*, "is a type of applied art where social science and mathematics are integrated to flesh out the strategic options within both the kinetic and non-kinetic approaches of a counterinsurgency campaign" (Morganthaler and Summers, 2011, p. 10). And this remains true, particularly with the issues confronted by the RTARF in southern Thailand. It is as much a non-kinetic approach as it is kinetic. With the insurgents' increased penetration and tight grip on the Malay-Muslim population, a more thorough understanding of the human terrain is required to devise strategic options that lead to a successful counterinsurgency operation.

SNA is accomplished using computer software such as NPS' Lighthouse application that provides analysis of patterns and relationship structures, using powerful algorithms that allow RTARF military planners to fully understand the inner workings of insurgent networks (Wellman, 2008, p. 222).

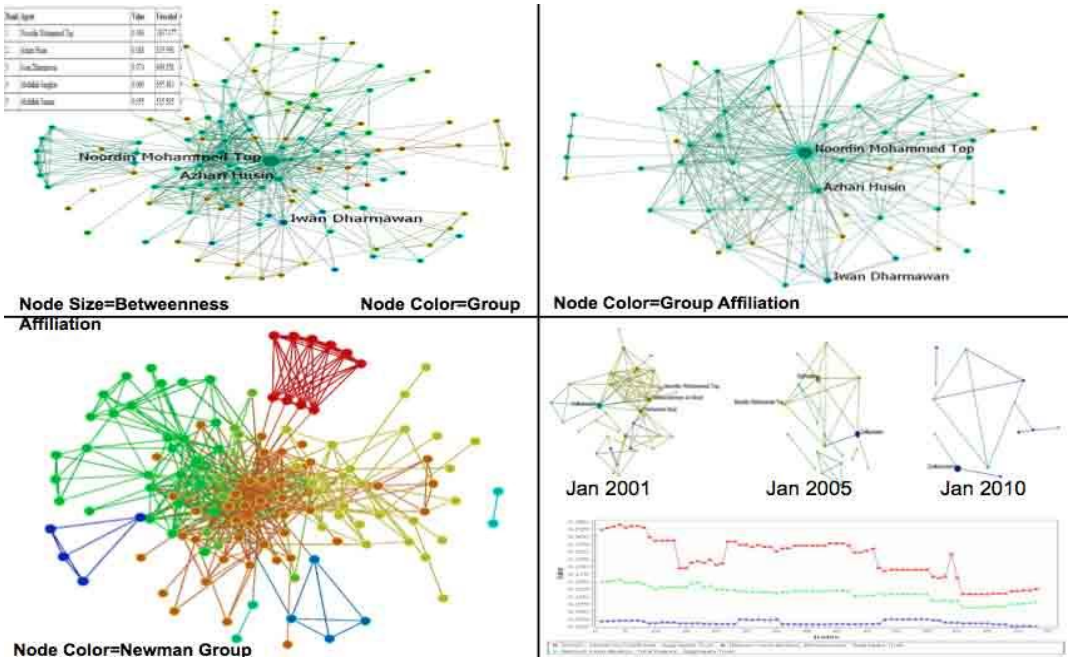

Figure 36. Lighthouse Social Network Visualization (from NPS CORE Lab)

One important aspect of modern SNA software is the ability to provide visualization of data collected mostly from human intelligence sources such as village surveys, interviews, informants and reconnaissance activities. The software generates a computer display (Figure 35) that can quantify the data and develop a clear operational picture that highlights the adversary's key social and organizational relationships, network structure, and potential weaknesses as well as vulnerabilities that can be exploited for future operations. Additionally, the software can also identify changes in the social network as operations are executed so metrics can be tracked to determine if a selected strategy's effectiveness. A constant reassessment of options based on evolving SNA data helps military commanders determine the appropriate course of action (McCormick, 2007, p.308).

(2) Geospatial Analysis

Geospatial analysis is defined by the National Geospatial-Intelligence Agency (NGA) as "the science of extracting meaning from geospatial data (information) and using geographic information systems (GIS) to uncover and investigate relationships and patterns to answer intelligence and military issues" (NGA, 2014). GIS is also defined by the NGA as "a computer-based, dynamic mapping system with spatial data-processing and querying capabilities" (NGA, 2014). GIS allows the problem solvers the data visualization of factors (Figure 36) affecting the problem to solve over the space. That visualization is given by mapping systematically the data to be analyzed.

Using geospatial analysis, military commanders are able to measure risks, to establish patterns, and with accurate information and methods, they can, to some degree, predict future situations by establishing "what if scenarios" with the purpose of being more proactive.

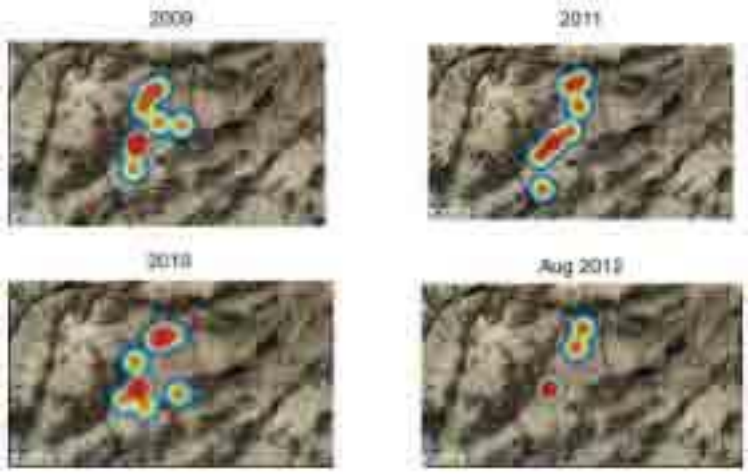

Figure 37. Lighthouse GIS visualization (from NPS CORE Lab)

Geospatial analysis and GIS play an important role in network centric operations. The integration of the geographic information about our own forces, the environment, and the enemy forces on the field is achieved by the implementation of a common GIS platform. Furthermore, the imagery collected by the sensors in the area of operations, and

the geospatial analysis deliver the required intelligence to provide an accurate "common picture" from the national down to the tactical level.

(3) Temporal Analysis

Temporal analysis is an important factor to consider in the GEOINT process as it provides an attempt to understand time patterns within collected data. This activity is often embedded in the geospatial analysis as time factor is a critical element into the whole analysis. It is difficult to talk about imagery, geospatial, and temporal analysis as separate entities, because they complement each other and are simply parts of the whole picture. In spite of the fact that an imagery product offers detailed information, when developing imagery analysis, it is still only a snapshot, a picture of a particular place at a particular time. Imagery is a static piece of intelligence, revealing something about where and when it was taken but nothing about what happened before and after.

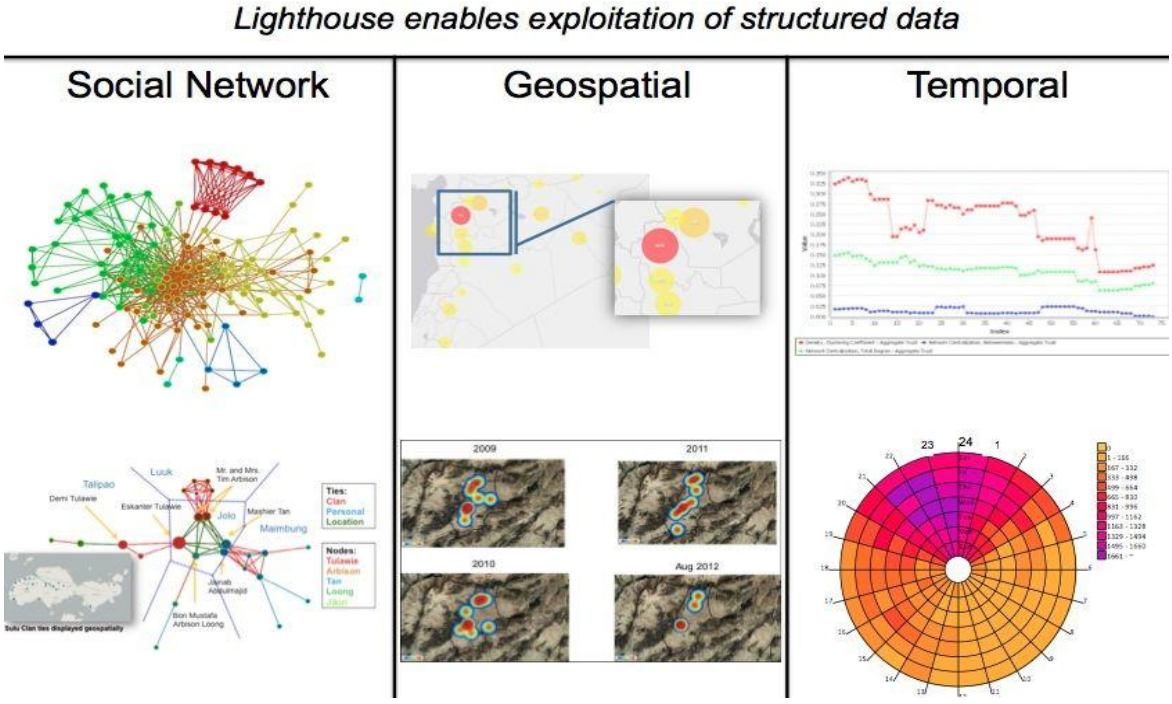

Figure 38. Lighthouse Analytical Components

b. Lighthouse Application

(1) Counter-Improvised Explosive Device (C-IED) Operations

At the heart of Lighthouse's C-IED methodology is a component known as IED Network Analysis (IEDNA). This application leverages mobile hand-held devices that allow rapid, streamlined, structured on-scene data collection. IEDNA also allows EOD operators to display guides to ordnance, homemade explosives components, tactics, techniques and procedures as soon as they arrive at the scene of an IED explosion, to get a better situational awareness and provide reporting accuracy.

To maximize the effectiveness of the Lighthouse application, the mobile devices require a network layer to transmit and receive data. During the Crimson Viper C-IED phase, the HFN wireless mesh was used to send data collected from the Hat Yao joint operations area to the IEDNA server at the NPS Core Lab in Monterey, California (Figure 38).

Figure 39. RTN EOD Personnel in Lighthouse C-IED Exercise

Using field data collected from Thailand, the IEDNA server was able to narrow the geographic interest by using a combination of social, temporal and geospatial analysis. The ability to state explicitly an area that needs to be scrutinized allows commanders to focus units and resources more effectively and accurately as opposed to covering a wide swath of territory without any assurance of success.

Figure 40. RTN EOD Collecting IED Data with Lighthouse Application

The C-IED phase of Crimson Viper demonstrated to the RTARF the effectiveness of network centric approach that leveraged both hardware (HFN) and software (Lighthouse) in resolving one of the more pressing issues in southern Thailand – the IED problem. It is also important to note that the limited analysis conducted has been performed without the benefit of human intelligence which is the main source of the RTARF's C-IED information.

(2) Village Stability Operations

Aside from C-IED operations, another component of a counterinsurgency campaign is village stability operations (VSO). Understanding the human terrain, requires a deep understanding of ethnic and tribal rivalries, local economy, influence of powerbrokers, and complex relationships within a village. The human domain is integral to population-centric conflicts such as the insurgency in southern Thailand and has a number of elements that extend beyond the physical environment. Understanding these elements is essential to VSO as it helps uncover the interconnected, socio-cultural network structure of local government officials, insurgents, other hostile elements, and other state and non-state actors.

Lighthouse technology can help support the RTARF in VSO by providing its troops with a tool that provides the means to map the human terrain with sociograms that allows for socio-cultural analysis. Sociograms are maps that depict social ties between nodes as a network. Each node represents an individual actor or another entity such as a

village, tribe, or group affiliation. Nodes are positioned in a "social space" so that in a particular visual representation the closer they are together, the more social ties or characteristics they have in common. Understanding these social ties is key to conceptualizing complex village dynamics in a VSO environment. With superior information and a better understanding of the human terrain in southern Thailand, the RTARF can effectively direct its resources in key villages that have a significant influence to the insurgency movement. This supports information operations (IO) such as civil-military engagements and psychological operations.

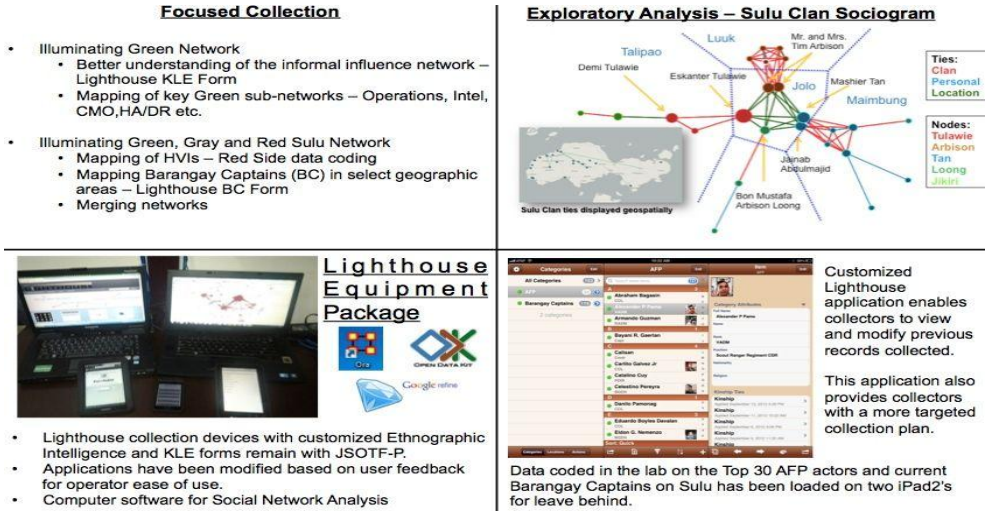

Figure 41. Lighthouse Key Components

(3) Rapid Information and Communication Technology Assessment

Information and Communication Technology (ICT) assessments are critical for military first responders that deploy in support of humanitarian assistance and disaster relief (HA/DR) missions after a major natural or man-made disaster. In most cases, the ICT infrastructure is often degraded to the point that first responders are unable to effectively coordinate efforts and prioritize response. The ability to thoroughly assess the ICT landscape enables responding organizations to reduce the communications gap so as provide a coordinated, multi-agency response effort.

Although not necessarily a direct function of a counterinsurgency operation, it is important to note that HA/DR missions are crucial to winning "hearts and minds" in disaster situations that may potentially occur in the insurgent infested areas of southern Thailand. The RTARF's ability to provide immediate and direct assistance to calamity victims will certainly provide a boost to government efforts in winning the population over.

The NPS Lighthouse application that is installed on mobile devices such as a cellphone or tablet computer can serve as a primary data collection tool that helps overcome the constraints associated with the initial chaos in the disaster aftermath. Integrated with HFN technology, Lighthouse can provide access to real-time data as well as geospatial analytics that helps provide targeted allocation of resources that results in a reduction of gaps and less duplication of effort which ultimately prevents additional loss of life, spread of disease and unnecessary suffering.

During the Crimson Viper technology demonstration, we conducted a three-day test of the Rapid Technology Assessment Team (RTAT) framework designed to conduct rapid ICT assessments. RTARF counterparts were trained on the use of the Lighthouse data collection/display tool at the joint operations area in Hat Yao, Thailand (Figure 41).

Figure 42. RTAT/ICT Training with RTARF Counterparts

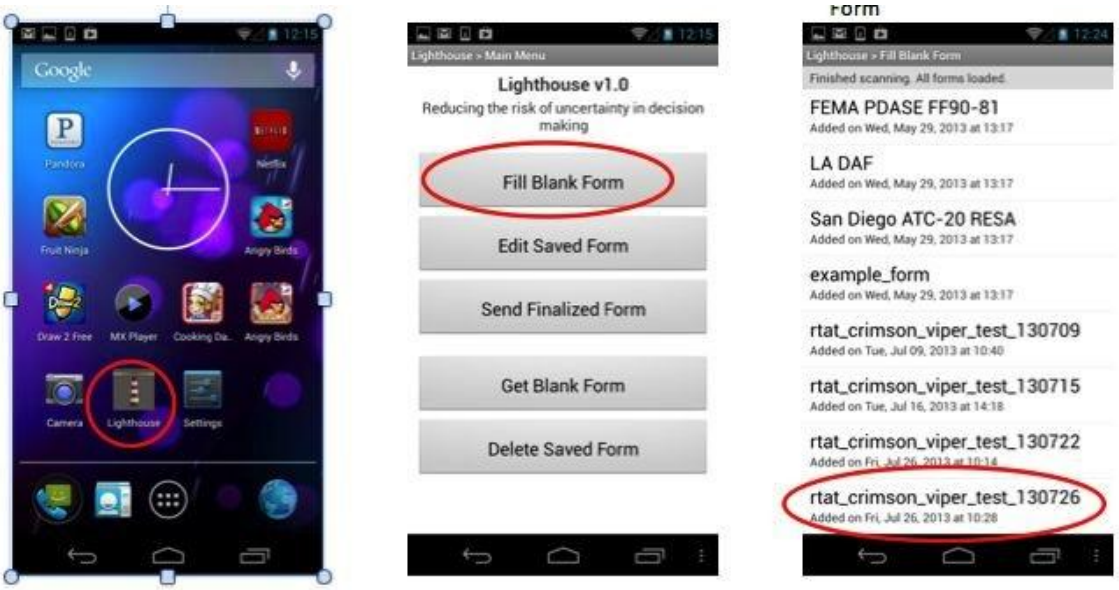

Figure 43. Lighthouse RTAT/ICT Screen Shot #1

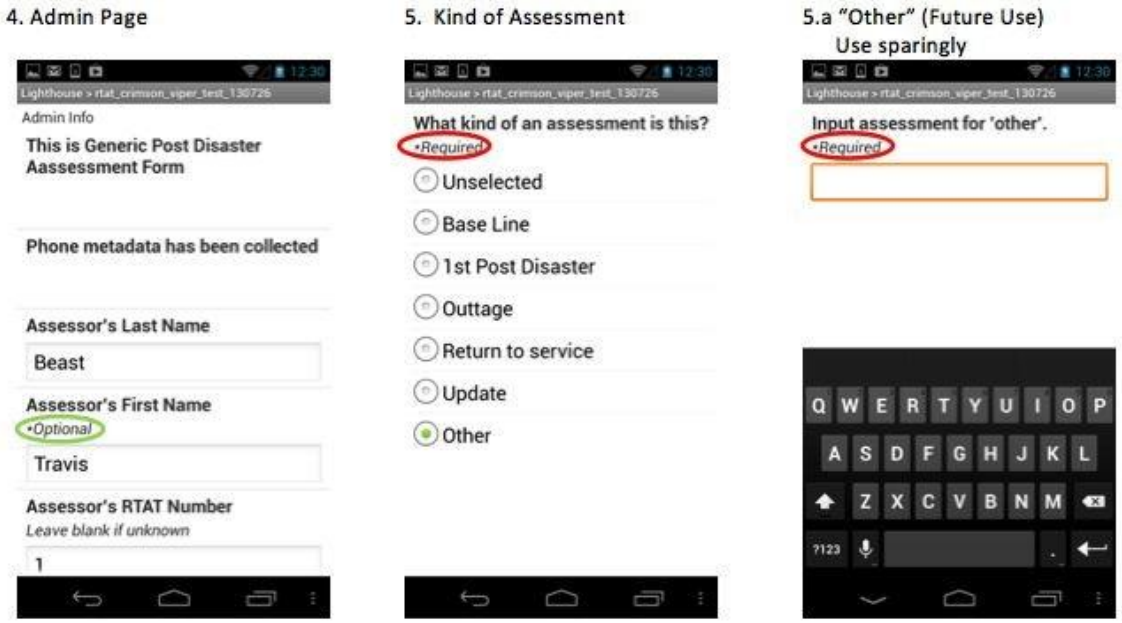

Figure 44. Lighthouse RTAT/ICT Screen Shot #2

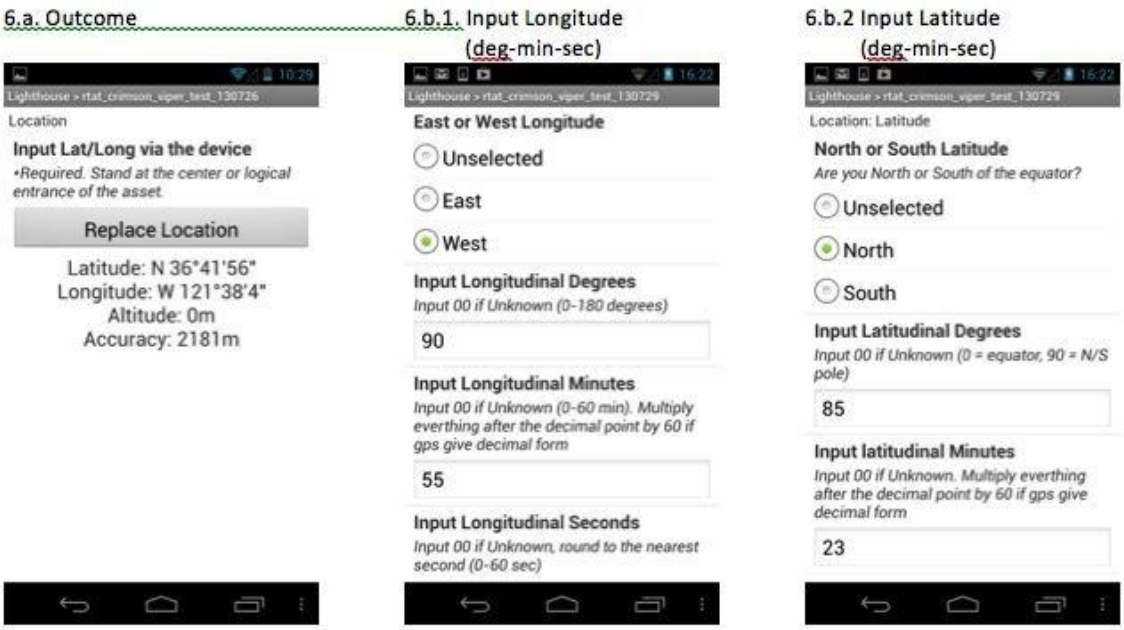

Figure 45. Lighthouse RTAT/ICT Screen Shot #3

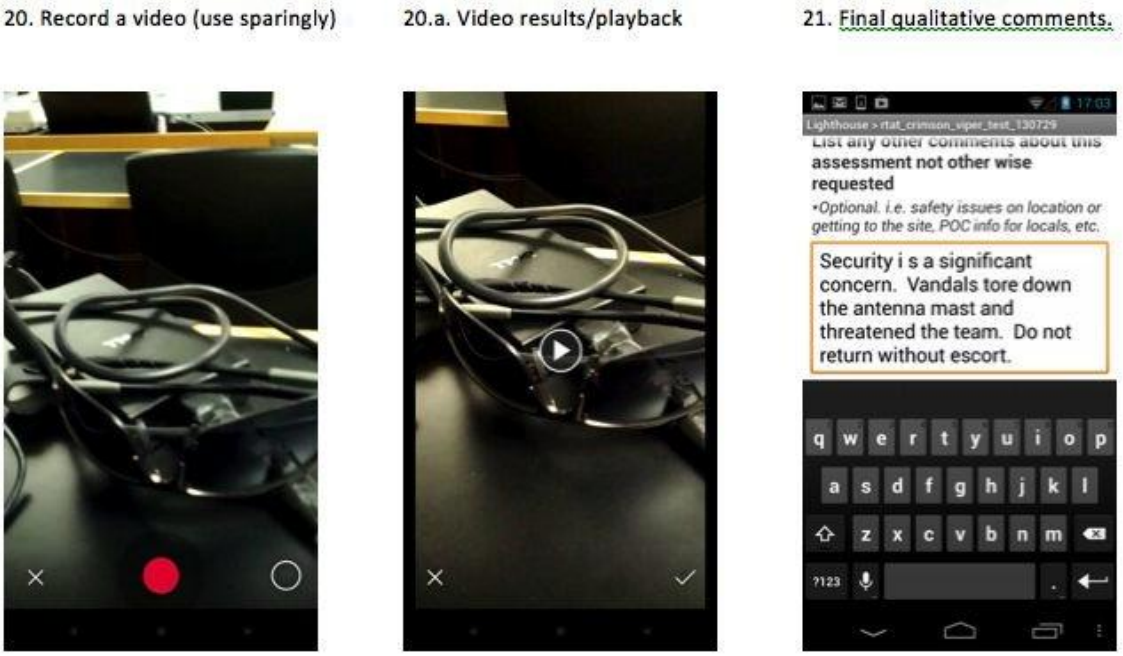

Figure 46. Lighthouse RTAT/ICT Screen Shot #4

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

Thailand's southern insurgency is not a conventional war; it is an asymmetric conflict that ascribes mainly to Mao Zedong's principles of popular protracted strategy. This approach leverages both the physical and human terrains found in rural environments. Despite this, the RTARF has employed a mainly conventional strategy that prevents it from acting swiftly, decisively, and appropriately against the insurgents.

Countering asymmetrical threats as they relate to internal security requires the ability to perform various roles with high speed, small size, and reliable technology. These asymmetrical threats potentially challenge traditional command and control when applied to modern communication and sensor technology. Therefore, emerging technologies linked via wireless networks present increased capabilities for RTARF's security forces deployed to remote areas of operation, and also help to facilitate shared situational awareness across the spectrum of combat. Additionally, non-state actors such as terrorists and insurgents have become more mobile, decentralized and sophisticated. Therefore, RTARF intelligence needs to transform its business processes and execute its intelligence activities in the most rapid and effective way possible, deviating from the traditional methods of relying solely on human intelligence (HUMINT) and a top-down staff approach to intelligence analysis. New capabilities that involve multi-source data collection, visualization methods and real-time information provide RTARF commanders with timely and accurate intelligence for supporting the final decision; this is a critical necessity to resolving the current insurgency situation in southern Thailand.

A new technological framework that integrates the components and principles of network centric warfare enables the RTARF to be more flexible in a constantly changing insurgent environment. This would not only give them a strategic and informational advantage over enemy forces but it would also reduce their uncertainty, which would release their warfighters from the fog and friction of war.

Network centric operations can be an expensive solution given the myriad of technologies that need to be implemented and integrated into current military operations.

The costs will largely depend on the level of complexity and technological sophistication that the RTARF wants to achieve. However, hastily formed networks (HFNs), in our opinion, meet the requirements in providing the RTARF with a cost-effective platform; the concept relies mainly on robust commercial off the shelf (COTS) technology that is relatively easy to deploy, operate and maintain.

Integrating currently fielded HFN solutions into RTARF's counter-insurgency operations would require little more than purchasing the known solutions and integrating them into existing infrastructure. UAV-mounted solutions that extend the range of communications are easily obtainable, although far less common—some amount of engineering would be required, but little more than fabricating mounting brackets for the correct fit and balance.

Military-grade UAVs used by the U.S. are prohibitively expensive, with typical system costs for a *Predator* exceeding $3.7 million. Use of the *Global Hawk* is even more prohibitive, with cost exceeding $15 million per airframe. This makes sourcing UAVs from commercially available sources not only desirable but also necessary.

Commercially available (or "professional" grade) solutions are globally available at a fraction of the cost of *Predators* or *Global Hawks*. Typical multi-rotor systems, capable of covering large distances and hovering for extended periods with large-capacity battery stores, cost under $10K for complete end-to-end solutions. GPS transponders, network equipment, and radios could be purchased and outfitted to these kinds of unit at reasonable cost. For a less robust but less costly system, "hobbyist" grade UAV solutions are available at the sub-$6K price range, with tracking and reporting hardware available for the price of a smartphone (which also include the advantage of considerably more well-supported software development environments).

An added benefit to employing HFNs and their enabling technologies is that they reduce the manpower required to accomplish the same mission. This translates into a smaller personnel footprint and ultimately less exposure for police and military forces to be placed in harm's way. Wireless mesh (WMN) and mobile ad hoc networks (MANET) provide the tactical networking framework for improved situational awareness and

information superiority through ubiquitous sharing of information including remote sensor and targeting data.

A. FUTURE RESEARCH

For a more complex system of UAV-based network nodes, it is recommended that further research be conducted that identifies most viable solutions based on several characteristics:

(1) UAV payload capacity

(2) Battery energy density and weight

(3) Lightweight solar paneling – for trickle charge and emergency recharge while landed outside a controlled area

(4) WiMax equipment (particularly comparing ranges vs. power consumption)

It is also recommended that additional UAV research be conducted in pursuit of designing a system that approaches UAV control as a one-to-many system; specifically, a system that requires only one pilot controlling a swarm of UAVs that have semi-autonomous capabilities. This concept, discussed in Chapter 4, would allow for considerable cost savings by reducing the number of personnel on station, and allow UAV onboard computer systems to react to network congestion, environmental, and adversarial related conditions faster than human response time would allow.

Research into UAV swarm management software should initially focus on potential trade-offs between time on station (for a static-hovering node configuration) and mobility time/range (for a more fluid rotating-node based configuration). The development of swarm management software should be a multi-disciplinary project, and it is recommended that the following areas be researched prior to designing and coding the controlling software:

Height-mapping algorithms using multiple sensor input (i.e., IR, high frequency audio echo, multiple offset image depth mapping, RADAR)— Altitude by altimeter will likely not be sufficient due to forest canopy environments; finding the most energy/cost efficient method of avoiding ground-based obstacles.

3-dimensional geographic positioning optimization algorithms based on GPS & relative signal strength of nearby nodes—the swarm should ideally share telemetry data from onboard sensors; developing the system in such a way that makes UAVs automatically reposition themselves based on other swarm member positions would significantly boost network fidelity and promote self-healing.

Use of Vertlet integration for predictive positional adjustments—typically used for simulations of molecular interactions or structural stress testing, an existing method of Vertlet integration could be used to detect changes in the swarm positional data and develop real-time predictive models to adjust swarm vectoring and preserve positional integrity (i.e., high winds begin moving swarm members, and the predictive model would allow swarm members not yet effected to compensate in advance of the wind).

It can be concluded that NPS' participation in the Crimson Viper 2013 technology demonstration provided insight to HFN and emerging technologies which may help fulfill the RTARF's requirement for a low- cost technological framework that helps address the existing information gap within its force structure that will ultimately lead to a successful counter-insurgency campaign in the Malay-Muslim regions of southern Thailand.

LIST OF REFERENCES

Abuza, Z.(2011). *The ongoing insurgency in Southern Thailand: Trends in violence, counterinsurgency operations, and the impact of national politics*. Washington, DC: Institute for National Strategic Studies.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network centric warfare: Developing and leveraging information superiority.* Washington, DC: DoD Office of Force Transformation.

Alberts, D. S. (2001). *Understanding Information Age warfare*. Washington, DC: CCRP Publication Series.

Ampunan, T. (2007). *The need for intelligence reform in Thailand's counterinsurgency*, (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA475905

Arugay, A.A. (2012). *The military along the security-development frontier: Implications for non-traditional security in the Philippines and Thailand*. Singapore: Center for Non-Traditional Security Studies. Retrieved from: http://www.rsis.edu.sg/nts/HTML-Newsletter/Report/pdf/NTS-Asia_Aries.pdf

Braun,T., Morgenthaler, S.,Zhao, Z., Staub, T. & Anwander, M. (2012). *UAVNet: A mobile wireless mesh network using unmanned aerial vehicles*. Bern, Switzerland: Institute of Computer Science and Applied Mathematics Universität Bern.

Byman, D. (2005). *Deadly connections: States that sponsor terrorism.* Cambridge: Cambridge University Press.

Cebrowski, A.K. (2002). *The implementation of network-centric warfare*. Washington, DC: DoD Office of Force Transformation.

Central Intelligence Agency (2012). *Guide to the analysis of insurgency.* Washington, DC: U.S. Government Printing Office.

Chalk, P. (2001). "Separatism and Southeast Asia: The Islamic factor in Southern Thailand, Mindanao and Aceh," *Studies in Conflict & Terrorism, 24* (24).

Chalk, P. (2008). *The Malay-Muslim Insurgency in Southern Thailand: Understanding the conflict's evolving dynamic*. Washington, DC: Rand. Retrieved from: http://www.rand.org/pubs/occasional_papers/OP198.html

Chatzigiannis, P., Gibson, J. H. & Singh, G. (2013).*Connecting Land-based Networks to ships*. (Master's thesis). Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/37462

Council of Foreign Relations. (2007). November 17, Revolutionary people's struggle, revolutionary struggle (Greece, leftists). Retrieved from: http://www.cfr.org/publication/9275

Crosson, B. (2010). Differences between secular insurgent groups. *Global Security Studies 1*(2). Retrieved from: http://globalsecuritystudies.com/Crosson%20Differences.pdf

Davis, A. (2004) Southern Thai insurgency gains fresh momentum. *Jane's Defense Intelligence Review*, *16*(8).

Everton, S.F. (2013). *Disrupting dark network,* Cambridge: Cambridge University Press.

Farouk, O. (1984). *The historical and transnational dimensions of Malay-Muslim separatism in Southern Thailand.* Singapore: Regional Strategic Studies Program, Institute of Southeast Asian Studies.

Hammes, T.X. (2004). *The sling and the stone: On war in the 21st Century*. Minneapolis, MN: Zenith Press.

Harish, S.P. (2006). Ethnic or religious cleavage: Investigating the nature of conflict in Southern Thailand. *Contemporary Southeast Asia*, 28 (1).

Hoffman, B. (2006). *Inside terrorism.* New York, NY: Columbia University Press.

Hubbard, F.R. (2002). *Model design for a battlegroup Intranet using a UAV.* (Master's thesis). Retrieved from: Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA401749

Human Rights Watch. (2007). Thailand's "war on drugs." Retrieved from: http://www.hrw.org/news/2008/03/12/thailand-s-war-drugs

Inmarsat Corp. Hughes 9201 BGAN Inmarsat Terminal Technical Specifications. Retrieved from: http://www.hughes.com/technologies/mobilesat-systems/mobile-satellite-terminals/hughes-9201-bgan-inmarsat-terminal/technical-specifications

Intel Corporation. (2005). 802.16 Wireless MAN specification accelerates wireless broadband access. Retrieved from: http://www.intel.com/technology/magazine/standards/st08031.pdf

Intel Corporation. (2005). Understanding Wi-Fi and WiMAX as Metro-Access Solutions. Retrieved from: http://www.intel.com/netcomms/technologies/wimax/304471.pdf

Internal Displacement Monitoring Center. (2011). *Conflict and displacement in Southern Thailand.* Retrieved from: http://www.internal-displacement.org/asia-pacific/thailand/2011/conflict-and-displacement-in-southern-thailand-november-2011

International Crisis Group. (2007). *Southern Thailand: Insurgency, not jihad* (Crisis Group Asia Report No. 98). Retrieved from: http://www.crisisgroup.org/~/media/Files/asia/south-east-asia/thailand/098_southern_thailand_insurgency_not_jihad.pdf

Janchitfah, S.(2005). *Violence in the mist: Reporting on the presence of pain in Southern Thailand*. Bangkok: Kobfai Publishing Project.

Jane's Intelligence Review. (2013) Growing pains: Malay-Muslim insurgency in Southern Thailand.

Klaimanee, W.(2008). *The need to improve population and resource control in Thailand's counterinsurgency* (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA494050

Kok, F. (2011). *Buddhist minority declines the "Deep South" due to protracted armed conflict*. Singapore: Internal Displacement Monitoring Center. Retrieved from: http://www.internal-displacement.org/assets/library/Asia/Thailand/pdf/201110-ap-thailand-overview-en.pdf

Kontogiannis, T. (2012). *Ad hoc sensor networks for maritime interdiction operations and regional security* (Master's thesis). Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/17389

Krishnamurthy, V. (2005). "Emission management for low probability intercept sensors in network centric warfare," *IEEE Transactions on Aerospace and Electronic Systems,* 23(2).

Leeper, D.G. (2005). "A long-term view of short-range wireless," *Computer,* 34 (6)

Lehr, W. & McKnight, L.W. (2005). Wireless Internet access: 3G vs. WiFi telecommunications policy. Retrieved from: http://pitpat.cs.utwente.nl/~draaijer/wifi/3G%20vs%20WiFi

Leifer, M. (1996). *A dictionary of the modern politics of South-East Asia*. New York, NY: Routledge.

Lim, M., Ng, N.M. & Yew, C. (2007). *An integrated architecture to Support Hastily Formed Networks* (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA475932

Lim, S.C. (2004). *Network centric warfare: A command and control perspective* (Master's thesis). Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/1656

Liow, J.C. (2004). *The security situation in Southern Thailand: Toward an understanding of domestic and international dimensions*. Singapore: Institute of Southeast Asian Studies.

Liow, J.C. (2009). *Islam, education and reform in Southern Thailand: Tradition and transformation dimensions*. Singapore: Institute of Southeast Asian Studies.

Lowenthal, M.M. (2006). *Intelligence: From secrets to policy.* Washington, DC: CQ Press.

Lucente, S. Wilson, G., Schroeder, R. & Freeman, G. (2013, April 1). "Examining social media and social network analysis for unconventional campaign planning." *Common Operational Research Environment Quarterly Newsletter*. Retrieved from: http://www.npscorelab.com/wp-content/uploads/April2013.pdf

Maisonti, T. (2004). *A proposal to address the emerging Muslim separatist problem in Thailand*. (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA429831

Matichon Daily News (2009). Southern crisis and daily violence report.

McCormick, G.H. & Giordano, F.(2007). "Things come together: Symbolic violence and guerrilla mobilization." *Third World Quarterly* 28 (2).

McCargo, D. (2008). *Tearing apart the land: Islam and legitimacy in Southern Thailand*. Ithaca, NY: Cornell University Press.

McKay, I. *An anarchist FAQ*. Retrieved from: http://www.infoshop.org/faq/intro.html, 2009.

McLean, I. & McMillan. (2009). *The Concise Oxford Dictionary of Politics*. (3rd ed.). Oxford, UK: Oxford Press.

Meillón, S.C. (2009). *Keeping current and increasing the effectiveness of the decision-making process and the interoperability in the Digital Age: Geospatial intelligence an geospatial information systems' applications in the military and intelligence fields for the Mexican Navy*. (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA493694

Menjivar, J.D. (2012). *Bridging operational and strategic communications: Integrating Small unmanned aircraft systems as airborne relay communication vertical nodes* (Master's thesis). Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/17418

Misra, S.C. & Woungang, I. (2009). *Guide to wireless sensor networks*. London: Springer.

Morganthaler, J., & Giles-Summers, B. (2011). *Targeting: Social network analysis in counter-IED operations*. (Master's thesis). Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/5703

Mkenology Blog. (2012). Malay Southern Thailand [Map]. Retrieved from http://www.mkenology.com/

National Council of Resistance of Iran (2009). Foreign Affairs Committee of the National Council of Resistance of Iran. Retrieved from: http://ncr-iran.org

National System for Geospatial Intelligence, *Geospatial Intelligence (GEOINT) basic doctrine.* Washington DC: U.S. National Geospatial-Intelligence Agency, 2014.

NIST. (2012). Wireless Ad-hoc sensor networks. Retrieved from: http://w3.antd.nist.gov/wahn_ssn.shtml

Noiwong, O. & Rubin, I. (2001). *Political integration policies and strategies of the Thai government towards the Malay Muslims of Southernmost Thailand* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database: http://search.proquest.com/docview/304716893

Ohrtman, F. (2005). Building 802.16 wireless networks. Retrieved from: http://www.techterms.com/definition/manet

O'Neill, B.E. (2005). *Insurgency and Terrorism—From Revolution to* Apocalypse (2nd ed.). Dulles, VA: Potomac Books.

Persistent Systems, *Technical Specifications for Wave Relay MPU4 and Quad Radio Router*. Retrieved from: http://www.persistentsystems.com/man-portable-unit-gen4/

Persistent Systems. Wave relay technical overview. Retrieved from: http://www.persistentsystems.com/pdf/PS_WaveRelay.pdf

Richardson, M. (1985). "Insurgency in the Philippines—The militia: help or hindrance." *Pacific Defence Reporter*, *12*(83).

Roberts, N. & Everton, S. (2013). "Strategies for combating dark networks," *Journal of Social Structure*, *12.*

Rodthong, C. (2009). *Balancing the direct and indirect approaches: Implications for ending the violence in Southern Thailand*. (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA514425

Royal Thai Air Force, RTAF's Operational Policy for Budget Year 2548

Sageman, M. (2004). *Understanding terror networks.* Philadelphia, PA: University of Pennsylvania Press.

Schumann, A. (2009). *Airborne ubiquitous surveillance and monitoring network.* (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA427211

Steckler, B. (2005). *Hastily Formed Networks for complex humanitarian disasters*. Retrieved from Calhoun, Institutional Archive of Naval Postgraduate School: http://hdl.handle.net/10945/37283

Thompson, E. (2013). U.S. Army harnesses sun to reduce casualties from sniper attacks. U.S. Army CERDEC Public Affairs.

Thuraya Inc. (n.d.). Thuraya IP plus technical specifications. Retrieved from: http://www.thuraya.com/thuraya-ip-plus

U.S. Department of Defense. (2002). Joint vision 2020 briefing. Retrieved from: http://www.dtic.mil/jointvision/jvpub2.htm

U.S. Department of Defense. (2005). Joint publication 1-02. Retrieved from: http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

U.S. Department of Homeland Security. (2005). *Study of terrorism and response to terrorism*. Retrieved from: http://www.start.umd.edu/data/tops/terrorist_organization_profile.asp?id=4072

Valentine, A. (2005). RTAF's "Ten Year Vision" translated by Albert Valentine. Retrieved from: http://www.admin.rtaf.mi.th/totalvision/cinc/rtaf1.htm

Valentine, A.R. (2005). *Leveraging Emerging Technologies in Southern Thailand* (Master's thesis). Retrieved from the Defense Technical Information Center website: http://www.dtic.mil/dtic/tr/fulltext/u2/a462701.pdf

Walgren, S.A. (2007). *Explaining intervention in Southeast Asia: A comparison of the Muslim Insurgencies in Thailand and the Philippines*. (Master's thesis). Retrieved from the Defense Technical Information Center website: http://handle.dtic.mil/100.2/ADA475791

Wellman, B, (2008). Review of the development of social network analysis: a study in the sociology of science. *Contemporary Sociology*, 37, pp. 221–222.

Wikipedia. (n.d.). Wireless ad-hoc network. Retrieved from: http://en.wikipedia.org/wiki/Wireless_ad-hoc_network, 2012.

Yegar, M. (2002). *Between integration and secession: The Muslim communities of the Southern Philippines, Southern Thailand and Western Burma/Myanmar*. New York, NY: Lexington Books.

Zimmerman, K. (2012). The Al Qaeda Network: A new framework for defining the enemy. Retrieved from: http://www.aei.org/files/2013/09/10/-the-al-qaeda-network-a-new-framework-for-defining-the-enemy_133443407958.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California